# FRAMEWORK SCHEDULE 2: SERVICES AND KEY PERFORMANCE INDICATORS

# PART A: SERVICES

## INTRODUCTION

* 1. The purpose of this Framework Schedule 2 is to provide a description of the Services that the Supplier shall deliver to the Contracting Authorities under the Lot-based structure of this Framework Agreement.
  2. The Services shall include:
* low volume work service packages;
* standard end-to-end service packages;
* individual Lot service packages; and
* high security end-to-end service packages.
  1. The Framework Agreement shall comprise of 9 Lots, as detailed in Section 3 – Lot Descriptions.

## PURPOSE

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

<http://www.edrm.net/resources/guides/edrm-framework-guides>

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 Agreement or Call Off Agreement, 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 Agreement span a wide and diverse customer base and require a variety of specialist services encompassed by the EDRM, but broadly some or all of the following eight (8) stages:
     1. Project Management and Advice;
     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 Agreement shall be structured to offer a Contracting Authority flexibility and choice. It shall be a matter of judgment for the Contracting Authority to decide which particular Lot(s) are most appropriate to meet with their specific requirements and best delivers their business need, and to ensure the most appropriate fit for the Contracting Authority’s requirements including value for money.

## LOT DESCRIPTIONS

* 1. A Contracting Authority 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 heading of the Lot). The Framework Agreement shall comprise of the following Lots:

|  |
| --- |
| **Lot 1 - 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 includes 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.  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 2: Services and Key Performance Indicators.  Mandatory requirements for **Lot 1** aredetailed at 4.4, 4.5, 4.6, 4.7, and 4.9 of this document:   * Document Processing, as detailed in paragraph 4.4; * Document Review, as detailed in paragraph 4.5; * Document Production, as detailed in paragraph 4.6; * Disclosure from Other Opponent Parties, as detailed in paragraph 4.7; and * Security Requirements, as detailed in paragraph 4.9 |
| **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 2: Services and Key Performance Indicators.  **ALL** of the Mandatory requirements relate to **Lot 2.**   * Project Management and Advice, as detailed in paragraph 4.1; * Document Identification, as detailed in paragraph 4.2; * Data Preservation and Collection, as detailed in paragraph 4.3; * Document Processing, as detailed in paragraph 4.4; * Document Review, as detailed in paragraph 4.5; * Document Production, as detailed in paragraph 4.6; * Disclosure from Other Opponent Parties, as detailed in paragraph 4.7; * Presentation at Trial, as detailed at paragraph 4.8; and * Security Requirements, as detailed in paragraph 4.9 |
| **Lot 3 - Project Management and Advice 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 2: Services and Key Performance Indicators.  Mandatory requirements for **Lot 3** aredetailed at 4.1 and 4.9 of this document:   * Project Management and Advice, as detailed at paragraph 4.1; and * Security Requirements, as detailed in paragraph 4.9 |
| **Lot 4 - Data Preservation and Collection 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 4,** as detailed in Section 4 of this Framework Schedule 2: Services and Key Performance Indicators.  Mandatory requirements for **Lot 4** are detailed at 4.3 and 4.9 of this document:   * Data Preservation and Collection, as detailed at paragraph 4.3; and * Security Requirements, as detailed in paragraph 4.9 |
| **Lot 5 - Document Processing 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 5,** as detailed in Section 4 of this Framework Schedule 2: Services and Key Performance Indicators.  Mandatory requirements for **Lot 5** are detailed at 4.4 and 4.9 of this document:   * Document Processing, as detailed at paragraph 4.4; and * Security Requirements, as detailed in paragraph 4.9 |
| **Lot 6 - Document Review and Document Production 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 6,** as detailed in Section 4 of this Framework Schedule 2: Services and Key Performance Indicators.  Mandatory requirements for **Lot 6** are detailed at 4.5 and 4.9 of this document:   * Document Review, as detailed at paragraph 4.5; * Document Production, as detailed at paragraph 4.6 and * Security Requirements, as detailed in paragraph 4.9 |
| **Lot 7 - Disclosure from Other Opponent Parties 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 7,** as detailed in Section 4 of this Framework Schedule 2: Services and Key Performance Indicators.  Mandatory requirements for **Lot 7** are detailed at 4.7 and 4.9 of this document:   * Disclosure from Other Opponent Parties, as detailed at paragraph 4.7; and * Security Requirements, as detailed in paragraph 4.9 |
| **Lot 8 - Presentation at Trial 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 8,** as detailed in Section 4 of this Framework Schedule 2: Services and Key Performance Indicators.  Mandatory requirements for **Lot 8** are detailed at 4.8 and 4.9 of this document:   * Presentation at Trial, as detailed at paragraph 4.8; and * Security Requirements, as detailed in paragraph 4.9 |
| **Lot 9 - 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 9,** as detailed in Section 4 of this Framework Schedule 2: Services and Key Performance Indicators.  **ALL** of the Mandatory requirements relate to **Lot 9**:   * Project Management and Advice, as detailed at paragraph 4.1; * Document Identification, as detailed at paragraph 4.2; * Data Preservation and Collection, as detailed at paragraph 4.3; * Document Processing, as detailed at paragraph 4.4; * Document Review, as detailed at paragraph 4.5; * Document Production, as detailed at paragraph 4.6; * Disclosure from Other Opponent Parties, as detailed at paragraph 4.7; * Presentation at Trial, as detailed at paragraph 4.8; and * Security Requirements, as detailed in paragraph 4.9 |

## 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 Period and until any Call Off Agreements established under this Framework Agreement expire.

* 1. **Project Management and Advice**
     1. The Supplier shall advise the Contracting Authority and its client in relation to the conduct of the disclosure exercise as a whole, including without limitation:
        1. how best to deal with the other parties’ disclosure;
        2. possible strategies for managing the overall exercise (as well as costs thereof), for example by way of ‘rolling disclosure’ or data sampling; and
        3. advice on the use of technologies and automation, including without limitation tools such as: analytics; predictive coding tools; and comparative software and tools.
     2. The Supplier may be required to attend and advise the Contracting Authority’s client at case management conferences, meetings or similar; for instance to assist with the completion of the Electronic Documents Questionnaire, found at the schedule to Practice Direction 31B of the CPR.
     3. The Supplier shall also assist with providing written statements and reports for the consideration of the court (or other relevant tribunals) as required.
     4. If required, the Supplier shall attend court (or other relevant tribunals) in person to give oral evidence.
     5. The Supplier shall provide overall project management (as opposed to concentrating only on deliverables and timelines), including ongoing budgetary management (such to also include regular analysis and reporting to the Contracting Authority 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).
  2. **Document Identification**
     1. In consultation with the Contracting Authority and their client, the Supplier shall conduct a proportionate exercise investigating and establishing an accurate picture of all the Contracting Authority’s client’s data sources (data mapping) including sources of hardcopy documents not otherwise held electronically.
     2. As advised by the Contracting Authority and their client, the Supplier shall identify potentially relevant ESI sources in relation to the information for proper and defensible completion (by the Contracting Authority and/or their client) of the Electronic Documents Questionnaire found at the schedule to Practice Direction 31B of the CPR, 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 Contracting Authority’s client;
        5. types of electronic mail servers used by the Contracting Authority’s client, 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 client, including digital voicemail stores, portable devices and mobile telephones, information stored on the Contracting Authority’s client’s intranet, instant messaging, and any other collaborative systems.
     3. As advised by the Contracting Authority and their client, the Supplier shall identify potentially relevant hardcopy document sources held by the Contracting Authority’s client, including investigation and consideration of:
        1. the Contracting Authority’s client’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 Contracting Authority’s client’s departmental filing;
        6. personal filing; and
        7. personal possession.
     4. The Supplier shall document the steps taken for the document identification phase, by way of a comprehensive report to the Contracting Authority and their client detailing compliance with the requirements of Part 31 of the CPR, which:
        1. satisfies them that the searches are evidenced by a clear audit trail, are reasonable and proportionate, and comply with the Contracting Authority’s client’s disclosure obligations; and
        2. recommends an early defensible and strategic approach to the collection, preservation, processing, review and production of the Contracting Authority’s client’s information, and includes initial indicative cost estimates and work timetables.
  3. **Data Preservation and Collection**
     1. The Supplier shall assist the Contracting Authority’s client to preserve all original potentially relevant data (hardcopy and electronic), for possible use in the litigation process.
     2. The Supplier shall assist the Contracting Authority’s client 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 Contracting Authority (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 Contracting Authority or their client department (as advised by the Contracting Authority); or
        2. if required, consolidating the data, including the option of doing so within a database store located on the Contracting Authority’s client’s premises.
     3. Where appropriate and if so instructed by the Contracting Authority, the Supplier shall also visit any site where their client’s data is held and conduct necessary inspections prior to the above activity.
     4. The Supplier shall assist the Contracting Authority’s client to securely acquire all potentially relevant hardcopy documents from the sources identified in the document identification phase or otherwise as instructed by the Contracting Authority, and take that material into the Supplier’s possession.
     5. The Supplier shall document the steps taken as above, by way of a comprehensive report to the Contracting Authority and their client 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 Contracting Authority’s client’s legal obligations.
  4. **Document Processing**
     1. The Supplier shall assess the data collected (whether by the Supplier as above or delivered by the Contracting Authority or their client) and report to the Contracting Authority and their client 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 Contracting Authority client’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 Contracting Authority and their client), 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 (de-duplication).
     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 Contracting Authority and their client, such to include at least the option of:
        1. pre-selected search terms and word strings (as advised by the Contracting Authority), to be applied across all prepared data;
        2. grouping documents which either:
     4. share 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. The Supplier shall within the output transform the data selected for review into a common format necessary for the downstream review platform to be used, whilst also retaining the data in its Native Form. This should include the following options (as elected by the Contracting Authority and their client) 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 Contracting Authority) of near-duplicates (near-duplication).
     9. The Supplier shall regularly analyse and validate data and results achieved, throughout all of the stages in the Document Processing phase, in order to ensure that overall results are as intended and handling decisions are correct and defensible.
     10. At the output stage the Supplier shall implement an appropriate quality assurance procedure that ensures that the proposed output meets initial expectations and that any significant variances from expectations are accounted for and explained.
     11. The Supplier shall document the steps taken for the Document Processing phase by way of a comprehensive report to the Contracting Authority and their client, 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 Contracting Authority client’s legal obligations.
  5. **Document Review**
     1. The Supplier shall support the Contracting Authority and their client 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 Contracting Authority 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 Contracting Authority 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.
   * + 1. if required, providing secure off-site hosting of data subject to the review process, and managing access thereto (whether remotely or otherwise);
       2. if required, provide technology-assisted review services in support of the review exercise, including at least the following:
     1. searching for and finding similar documents based on a ‘seed’ document set;
     2. analytics including visual analysis of data;
     3. mapping the way the other parties in the dispute worked;
     4. concept clustering;
     5. identifying an absence of information;
     6. prioritising responsive documents; and
     7. identifying behaviors (e.g. fraudulent, negligent, incompetent conduct).
        1. if required, to provide suitable legally-qualified (graduate level) reviewers to undertake first pass review, including management of those reviewers and the first pass review exercise.
     8. The Supplier shall document the steps taken for the Document Review phase by way of a comprehensive report to the Contracting Authority and their client, 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 Contracting Authority’s client’s legal obligations.
   1. **Document Production**
      1. The Supplier shall advise and assist the Contracting Authority and their client with producing disclosure lists 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 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. 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;
4. ‘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;
5. production of disclosable hard copy documents in hardcopy form, including an ability to prepare indexed and paginated hardcopy document bundles; and
6. 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.
   * 1. The Supplier shall document the steps taken for the Production phase by way of a comprehensive report to the Contracting Authority and their client 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 Contracting Authority’s client’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 Contracting Authority’s client’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**
      1. The Supplier shall also be required to provide the following Services in respect of receipt of disclosure documents from other parties (by the Contracting Authority), 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;
         2. assess the data received and report to the Contracting Authority and their client regarding precisely what data has been received (including data size and type), possible complications or problems and recommend strategies for overcoming them;
         3. advise and recommend strategies for review, and then implement such strategies in a manner agreed with the Contracting Authority and their client, such strategies to include:
      3. preparation of the data for review, including at least the following options:
7. identifying and eliminating duplicates (de-duplication), if any;
8. applying pre-selected search terms and word strings (as advised by the Contracting Authority) across all prepared data;
9. grouping documents which either share common concepts or were created at a particular time or by a particular individual or group of individuals;
10. linking email chains to result in a continuous email exchange from first to last email, across multiple users;
11. linking any other data threads generally (and recording any relevant audit information that may be available);
12. cross-referencing documents from different parties with a view to performing searches across responses;
13. relevance ranking; and
14. identification of near-duplicates in accordance with parameters set by the Contracting Authority (near- duplication).
    * 1. 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.
      2. 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.
      3. 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.
      4. The Supplier shall document the steps taken by way of a comprehensive report to the Contracting Authority and their client, detailing compliance with the requirements of Part 31 of the CPR, 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 Contracting Authority and their client to properly and effectively review the other litigants’ disclosure.
      5. The Supplier shall provide document review support to the Contracting Authority and their client 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 Contracting Authority’s premises, their client’s premises, or premises provided by the Supplier, such software to allow for:
      6. lawyer review of the other parties’ disclosure, and selection of individual documents for further consideration; and
      7. 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. if required, providing and supporting necessary hardware (for example document review workstations) for use in the review process at the Contracting Authority’s premises, their client’s premises, or premises provided by the Supplier, together with the aforementioned software;
         2. if required, providing secure off-site hosting of data subject to review, and managing access thereto (whether remotely or otherwise).
      8. The Supplier shall document the steps taken by way of a comprehensive report to the Contracting Authority and their client 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**
     1. The Supplier shall assist with the presentation of ESI or hardcopy documents at court (or other relevant tribunals) as directed by the Contracting Authority. 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 Contracting 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 Contracting Authority’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 Contracting Authority.
  2. **Security Requirements**
     1. The Supplier shall comply with the security requirements contained within Annexes 1 and/or 2, as appropriate. For the avoidance of doubt, where material being handled under Lot 9 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 2 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 – 8)

## INTRODUCTION

* 1. These security requirements apply in respect of all e-Disclosure exercises called- off and conducted under this Framework Agreement, such always being exercises where the Contracting Authority’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 Agreement and any Call-Off Agreements, to provide Services that comply with the following:
     1. legislation:
        1. Data Protection Act 1998
        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):

[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](https://www.ncsc.gov.uk/guidance/browser-security-guidance)

* 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 Agreement, 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 Contracting Authority and/or their client to be particularly sensitive, the Supplier may be required to enter into further consultation with the Contracting Authority and/or their client’s security personnel to agree additional minimum controls.

## GOVERNANCE REQUIREMENTS

* 1. The Supplier shall be accredited to (and remain so accredited throughout the duration of this Framework Agreement and all Call-Off Agreements) Information Security Management System ISO 27001:2013 or equivalent, confirming that their IT systems/service including the segment that delivers e-Disclosure Services to the Contracting 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, for the duration of the Framework Agreement and any Call-Off Agreements, also present a current and valid Cyber Essentials certificate which has been awarded by one of the government approved Cyber Essentials accreditation bodies within the most recent 12 months.
  3. Alternatively, the Supplier shall, for the duration of the Framework Agreement and any Call-Off Agreements, be accredited to Information Security Management System ISO 27001:2013 or equivalent ISO27001 standard where the Cyber Essentials requirements have been included in the scope of that standard, and verified as such and the certification body carrying out this verification is approved to issue a Cyber Essentials certificate by one of the government approved Cyber Essentials accreditation bodies.

## REQUIRED OPERATIONAL ENVIRONMENT FOR OFFICAL 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 Contracting Authority’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 Contracting Authority shall advise the Supplier of such requirements in advance. This information is likely to be in Annex 3 of the contract agreement. Any solution or Service will be individually accredited by the Contracting Authority 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 [Cloud](https://www.gov.uk/government/collections/cloud-security-guidance) [Security](https://www.ncsc.gov.uk/guidance/cloud-security-collection) [Principles](https://www.gov.uk/government/collections/cloud-security-guidance), to demonstrate end-to-end protection. Where the use of a cloud service imposes a specific security requirement, 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 Communications-Electronics Security Group (“CESG”) published guidance [End](https://www.gov.uk/government/publications/end-user-devices-security-principles) [User](https://www.ncsc.gov.uk/guidance/end-user-device-security) [Devices Security Principles](https://www.gov.uk/government/publications/end-user-devices-security-principles) 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).

## 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:

1. Vulnerability management (patch management):
2. 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 mitigatory action (e.g. patch applied) shall be taken immediately.
3. Where a Supplier is unable to deploy a patch within the above minimum timescales then the Supplier shall take alternative mitigatory 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. Protective monitoring and intrusion detection:
9. 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 Contracting Authority on demand.
10. 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.
11. 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.
12. Security incident response:
13. 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 Further Competition conducted under this Framework Agreement to the Contracting Authority as soon as possible.
14. 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 Contracting Authority on demand.
15. In the event of an incident the Supplier shall provide the Contracting Authority with audit logs holding user activities, exceptions and information security events to assist in investigations.
16. 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.

## AUTHENTICATION AND ACCESS CONTROL

* 1. The Supplier shall ensure that accounts are provisioned with privileges appropriate for the user need. 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 ‘[Password Guidance: Simplifying Your Approach](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/458857/Password_guidance_-_simplifying_your_approach.pdf)’:

1. ensure that all passwords are changed from defaults;
2. not allow password/account sharing;
3. ensure that high-privilege users (i.e. administrators) use different passwords for their high-privilege and low-privilege accounts;
4. combine passwords with some other form of strengthening authentication, such as lockouts, throttling or two-factor authentication;
5. 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)

## 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 Contracting Authority 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 (Contracting Authority 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.

**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.

## 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](C:\\Users\\rebecca.vare\\Downloads\\cloud security principles)

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.

## SEPARATION of SERVICES

* 1. The Supplier shall ensure that the Contracting Authority’s data is separate from other customers data hosted on the same infrastructure.

**ANNEX 2**

**INFORMATION SECURITY REQUIREMENTS FOR e-DISCLOSURE EXERCISES UP TO ‘SECRET’ AND ‘TOP SECRET’ CLASSIFICATION (Lot 9 only)**

1. **INTRODUCTION**
   1. These security requirements apply in respect of all eDisclosure exercises called-off and conducted under Lot 9 of this Framework Agreement, such always being exercises where the Contracting Authority’s mitigating measures are influenced by the current and previous HMG protective marking schemes. This Annex 2 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 Agreement and any Call-Off Agreements, to provide Services that comply with the following:
      1. legislation:
         1. Data Protection Act 1998
         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):

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

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

[Browser Security](https://www.ncsc.gov.uk/guidance/browser-security-guidance);

[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 Agreement, 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 Contracting Authority and / or their client to be particularly sensitive, the Supplier may be required to enter into further consultation with the Contracting Authority 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 Agreement and all Call Off Agreements) Information Security Management System ISO 27001:2013 or equivalent, confirming that their IT systems/service including the segment that delivers eDisclosure Services to the Contracting 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 Agreement and any Call-Off Agreements, a current and valid Cyber Essentials certificate or equivalent, which has been awarded by one of the government approved Cyber Essentials accreditation bodies within the most recent 12 months.
   3. Alternatively, the Supplier shall, for the duration of the Framework Agreement and any Call-Off Agreements, be accredited to Information Security Management System ISO 27001:2013 or equivalent ISO27001 standard where the Cyber Essentials requirements have been included in the scope of that standard, and verified as such and the certification body carrying out this verification is approved to issue a Cyber Essentials certificate by one of the government approved Cyber Essentials accreditation bodies.
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 eDisclosure exercise: a Supplier-hosted closed network service with no internet access, and a Supplier closed network service hosted at the Contracting Authority 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 Contracting Authority shall advise the Supplier of these specific handling caveats. Any solution or Service will be individually accredited by the Contracting Authority 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, and PCs - connecting to their Services meets the relevant information security standards set out below, and in so doing should have specific reference to CESG’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 30 days and other vulnerabilities within 60 days. Where the Supplier knows that a vulnerability is being actively exploited then mitigatory 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 mitigatory 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>

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 Contracting Authority 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 Further Competition conducted under this Framework Agreement to the Contracting Authority 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 Contracting Authority on demand.
7. In the event of an incident the Supplier shall provide the Contracting Authority 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 need. 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 encryption of PCs or IT equipment on closed 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 Services. The Supplier’s crypto custodian shall manage this process. For passwords, the Supplier shall, with reference to CESG’s published best practice ‘[Password Guidance: Simplifying Your Approach](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/458857/Password_guidance_-_simplifying_your_approach.pdf)’:
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 Contracting 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 Contracting Authority’s IT systems and data are on stand-alone systems not shared with other customers data hosted on the same infrastructure.