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

# Order Form

CALL-OFF REFERENCE: RM6175-2024-1059841

PROJECT REFERENCE (Internal Reference) - prj_1489

| | |
|---|---|
| THE BUYER: | The Department for Energy Security & Net Zero (DESNZ) |
| BUYER ADDRESS | 3-8 Whitehall Place, London, SW1A 2EG |
| THE SUPPLIER: | Iron Mountain (UK) PLC |
| SUPPLIER ADDRESS: | Ground Floor, 4 More London Riverside, London, United Kingdom, SE1 2AU |
| REGISTRATION NUMBER: | 01478540 |
| DUNS NUMBER: | 227294949 |

APPLICABLE FRAMEWORK CONTRACT

This Order Form is for the provision of the Call-Off Deliverables and dated 01st September 2024
It's issued under the Framework Contract with the reference number RM6175 for the provision of British Coal Records Management.

CALL-OFF LOT(S):
***Records Information Management, Digital Solutions and Associated Services framework (RM6175 – Lot 5)***

CALL-OFF INCORPORATED TERMS
The following documents are incorporated into this Call-Off Contract. Where numbers are missing we are not using those schedules. If the documents conflict, the following order of precedence applies:

1. This Order Form including the Call-Off Special Terms and Call-Off Special Schedules.
2. Joint Schedule 1(Definitions and Interpretation) **RM6175**
3. The following Schedules in equal order of precedence:

   - Joint Schedules for **RM6175**
     - Joint Schedule 2 (Variation Form)
     - Joint Schedule 3 (Insurance Requirements)
     - Joint Schedule 4 (Commercially Sensitive Information)
     - Joint Schedule 6 (Key Subcontractors)
     - Joint Schedule 10 (Rectification Plan)
     - Joint Schedule 11 (Processing Data)
     - Joint Schedule 13 (Continuous Improvement)
     - Joint Schedule 14 (Benchmarking)

   - Call-Off Schedules for **RM6175**
     - Call-Off Schedule 1 (Transparency Reports)
     - Call-Off Schedule 2 (Staff Transfer)
     - Call-Off Schedule 5 (Pricing Details)
     - Call-Off Schedule 6 (ICT Services)
     - Call-Off Schedule 8 (Business Continuity and Disaster Recovery)
     - Call-Off Schedule 9 (Security)
     - Call-Off Schedule 10 (Exit Management)
     - Call-Off Schedule 13 (Implementation Plan and Testing)
     - Call-Off Schedule 14 (Service Levels)
     - Call-Off Schedule 15 (Call-Off Contract Management)
     - Call-Off Schedule 20 (Call-Off Specification)
     - Call-Off Schedule 24 (Supplier Furnished Terms)

4. CCS Core Terms (version 3.0.10)
5. Joint Schedule 5 (Corporate Social Responsibility) **RM6175**
6. Call-Off Schedule 4 (Call-Off Tender) as long as any parts of the Call-Off Tender that offer a better commercial position for the Buyer (as decided by the Buyer) take precedence over the documents above.

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

CALL-OFF SPECIAL TERMS
The following Special Terms are incorporated into this Call-Off Contract:

See Call-Off Schedule 24 (Supplier Furnished Terms)

CALL-OFF START DATE: **01/09/2024**

CALL-OFF EXPIRY DATE: **31/08/2028**

CALL-OFF INITIAL PERIOD: 4 years 0 months

CALL-OFF DELIVERABLES

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

MAXIMUM LIABILITY
The limitation of liability for this Call-Off Contract is stated in Clause 11.2 of the Core Terms.

The Estimated Year 1 Charges used to calculate liability in the first Contract Year is **£580,000** in the first 12 months of the Contract.

CALL-OFF CHARGES

See details in Call-Off Schedule 5 (Pricing Details)]
All changes to the Charges must use procedures that are equivalent to those in Paragraphs 4, 5 and 6 (if used) in Framework Schedule 3 (Framework Prices)]

REIMBURSABLE EXPENSES
None

PAYMENT METHOD
[redacted]

BUYER'S INVOICE ADDRESS:

[redacted]

[redacted]

BUYER'S AUTHORISED REPRESENTATIVE
Head of Coal Liabilities Unit & Sponsorship Team

BUYER'S CONTRACT MANAGER

Assistant Head, Coal Liabilities Unit

BUYER'S SECURITY POLICY
Appended at Call-Off Schedule 9

SUPPLIER'S AUTHORISED REPRESENTATIVE
[redacted]

Strategic Account Manager

Ground Floor, 4 More London Riverside, London, SE1 2AU

SUPPLIER'S CONTRACT MANAGER
[redacted]

Sector Head

Ground Floor, 4 More London Riverside, London, SE1 2AU

PROGRESS REPORT FREQUENCY
On the first Working Day of each calendar month

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

KEY STAFF
[redacted]

Strategic Account Manager

Ground Floor, 4 More London Riverside, London, SE1 2AU

KEY SUBCONTRACTOR(S)
**N/A**

COMMERCIALLY SENSITIVE INFORMATION

Supplier's Commercially Sensitive Information set out in Joint Schedule 4 (Commercially Sensitive Information)

SERVICE CREDITS
Not applicable.

ADDITIONAL INSURANCES
Not applicable

GUARANTEE
Not applicable

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

| **For and on behalf of the Supplier:** | | **For and on behalf of the Buyer:** | |
|---|---|---|---|
| Signature: | [redacted] | Signature: | [redacted] |
| Name: | | Name: | |
| Role: | | Role: | |
| Date: | | Date: | |

# Joint Schedule 1 (Definitions)

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

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

1.3 In each Contract, unless the context otherwise requires:

1.3.1 the singular includes the plural and vice versa;

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

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

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

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

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

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

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

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

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

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

1.3.12 where the Buyer is a Central Government Body it shall be treated as contracting with the Crown as a whole;

1.3.13 any reference in a Contract which immediately before Exit Day is a reference to (as it has effect from time to time):

(a) any EU regulation, EU decision, EU tertiary legislation or provision of the EEA agreement ("**EU References**") which is to form part of domestic law by application of section 3 of the European Union (Withdrawal) Act 2018 shall be read on and after Exit Day as a reference to the EU References as they form part of domestic law by virtue of section 3 of the European Union (Withdrawal) Act 2018 as modified by domestic law from time to time; and

(b) any EU institution or EU authority or other such EU body shall be read on and after Exit Day as a reference to the UK institution, authority or body to which its functions were transferred; and

1.3.14 unless otherwise provided, references to "**Buyer**" shall be construed as including Exempt Buyers; and

1.3.15 unless otherwise provided, references to "**Call-Off Contract**" and "**Contract**" shall be construed as including Exempt Call-off Contracts.

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

| | |
|---|---|
| **Absolute Exemption** | means if information is captured by one of these there is no obligation under the Freedom of Information Act for the Buyers to release the Sensitive information identified within the Record and is therefore not subject to undertaking the Public Interest Test. |
| **Account Management** | means the Supplier's nominated person who is responsible for ensuring the successful delivery of Suppliers Record Management Service to Buyers. |
| **Achieve** | in respect of a Test, to successfully pass such Test without any Test Issues and in respect of a Milestone, the issue of a Satisfaction Certificate in respect of that Milestone and "**Achieved**", "**Achieving**" and "**Achievement**" shall be construed accordingly; |
| **Action Plan** | means a document that lists what steps must be taken in order to achieve a specific goal. The purpose of an Action Plan is to clarify what resources are required to reach the goal, formulate a timeline for when specific tasks need to be completed and determine what resources are require. |
| **Active Records** | means a Record which is still actively being used and are usually referenced to on a daily or monthly basis. |
| **Appraisal and Selection** | means the identification of Records containing historical information and selecting those Records for permanent preservation |

| | |
|---|---|
| **Additional Insurances** | insurance requirements relating to a Call-Off Contract specified in the Order Form additional to those outlined in Joint Schedule 3 (Insurance Requirements); |
| **Admin Fee** | means the costs incurred by CCS in dealing with MI Failures calculated in accordance with the tariff of administration charges published by the CCS on: http://CCS.cabinetoffice.gov.uk/i-am-supplier/management-information/admin-fees; |
| **Affected Party** | the Party seeking to claim relief in respect of a Force Majeure Event; |
| **Affiliates** | in relation to a body corporate, any other entity which directly or indirectly Controls, is Controlled by, or is under direct or indirect common Control of that body corporate from time to time; |
| **Annex** | extra information which supports a Schedule; |
| **Approval** | the prior written consent of the Buyer and "**Approve**" and "**Approved**" shall be construed accordingly; |
| **Audit** | the Relevant Authority's right to:<br>a) verify the accuracy of the Charges and any other amounts payable by a Buyer under a Call-Off Contract (including proposed or actual variations to them in accordance with the Contract);<br>b) verify the costs of the Supplier (including the costs of all Subcontractors and any third party suppliers) in connection with the provision of the Services;<br>c) verify the Open Book Data;<br>d) verify the Supplier's and each Subcontractor's compliance with the applicable Law;<br>e) identify or investigate actual or suspected breach of Clauses 27 to 33 and/or Joint Schedule 5 (Corporate Social Responsibility), impropriety or accounting mistakes or any breach or threatened breach of security and in these circumstances the Relevant Authority shall have no obligation to inform the Supplier of the purpose or objective of its investigations;<br>f) identify or investigate any circumstances which may impact upon the financial stability of the Supplier, any Guarantor, and/or any Subcontractors or their ability to provide the Deliverables;<br>g) obtain such information as is necessary to fulfil the Relevant Authority's obligations to supply information for parliamentary, ministerial, judicial or administrative purposes including the supply of information to the Comptroller and Auditor General; |

| | |
|---|---|
| | h) review any books of account and the internal contract management accounts kept by the Supplier in connection with each Contract;<br>i) carry out the Relevant Authority's internal and statutory audits and to prepare, examine and/or certify the Relevant Authority's annual and interim reports and accounts;<br>j) enable the National Audit Office to carry out an examination pursuant to Section 6(1) of the National Audit Act 1983 of the economy, efficiency and effectiveness with which the Relevant Authority has used its resources; or<br>k) verify the accuracy and completeness of any Management Information delivered or required by the Framework Contract; |
| **Auditor** | a) the Buyer's internal and external auditors;<br>b) the Buyer's statutory or regulatory auditors;<br>c) the Comptroller and Auditor General, their staff and/or any appointed representatives of the National Audit Office;<br>d) HM Treasury or the Cabinet Office;<br>e) any party formally appointed by the Buyer to carry out audit or similar review functions; and<br>f) successors or assigns of any of the above; |
| **Authority** | CCS and each Buyer; |
| **Authority Cause** | any breach of the obligations of the Relevant Authority or any other default, act, omission, negligence or statement of the Relevant Authority, of its employees, servants, agents in connection with or in relation to the subject-matter of the Contract and in respect of which the Relevant Authority is liable to the Supplier; |
| **BACS** | the Bankers' Automated Clearing Services, which is a scheme for the electronic processing of financial transactions within the United Kingdom; |
| **Beneficiary** | a Party having (or claiming to have) the benefit of an indemnity under this Contract; |
| **Bulk** | means a large amount of Records or Data |
| **Bulk Scanning** | means an agreement between Buyers and the Supplier to undertake specified Scanning project within a specified timeframe. |
| **Buyer** | the relevant public sector purchaser identified as such in the Order Form; |

| | |
|---|---|
| **Buyer Assets** | the Buyer's infrastructure, data, software, materials, assets, equipment or other property owned by and/or licensed or leased to the Buyer and which is or may be used in connection with the provision of the Deliverables which remain the property of the Buyer throughout the term of the Contract; |
| **Buyer Authorised Representative** | the representative appointed by the Buyer from time to time in relation to the Call-Off Contract initially identified in the Order Form; |
| **Buyer Premises** | premises owned, controlled or occupied by the Buyer which are made available for use by the Supplier or its Subcontractors for the provision of the Deliverables (or any of them); |
| **Call-Off Contract** | the contract between the Buyer and the Supplier (entered into pursuant to the provisions of the Framework Contract), which consists of the terms set out and referred to in the Order Form; |
| **Call Off Contract Manager** | means the Supplier's Contract Manager appointed to manage the Buyer's contract. |
| **Call-Off Contract Period** | the Contract Period in respect of the Call-Off Contract; |
| **Call-Off Expiry Date** | the scheduled date of the end of a Call-Off Contract as stated in the Order Form; |
| **Call-Off Incorporated Terms** | the contractual terms applicable to the Call-Off Contract specified under the relevant heading in the Order Form; |
| **Call-Off Initial Period** | the Initial Period of a Call-Off Contract specified in the Order Form; |
| **Call-Off Optional Extension Period** | such period or periods beyond which the Call-Off Initial Period may be extended as specified in the Order Form; |
| **Call-Off Procedure** | the process for awarding a Call-Off Contract pursuant to Clause 2 (How the contract works) and Framework Schedule 7 (Call-Off Award Procedure); |
| **Call-Off Special Terms** | any additional terms and conditions specified in the Order Form incorporated into the applicable Call-Off Contract; |
| **Call-Off Start Date** | the date of start of a Call-Off Contract as stated in the Order Form; |
| **Call-Off Tender** | the tender submitted by the Supplier in response to the Buyer's Statement of Requirements following a Further Competition Procedure and set out at Call-Off Schedule 4 (Call-Off Tender); |
| **Cataloguer** | means Supplier Personnel which shall extract information from a specific Record bringing to a specific standard and determining the description for a Record from which |

| | |
|---|---|
| | Metadata can be searched later using descriptions from within catalogues. |
| **Cataloguer Project Manager** | means the Project Manager who oversees the Cataloguer |
| **Catalogue Service Cataloguing Service** | means the process of extracting information form a specific Record and bringing a listing to a specific standard, determining a description for that Record from which metadata can then be searched later using descriptions and titles. |
| **CCS** | the Minister for the Cabinet Office as represented by Crown Commercial Service, which is an executive agency and operates as a trading fund of the Cabinet Office, whose offices are located at 9th Floor, The Capital, Old Hall Street, Liverpool L3 9PP; |
| **CCS Authorised Representative** | the representative appointed by CCS from time to time in relation to the Framework Contract initially identified in the Framework Award Form; |
| **Central Government Body** | a body listed in one of the following sub-categories of the Central Government classification of the Public Sector Classification Guide, as published and amended from time to time by the Office for National Statistics:<br>a) Government Department;<br>) Non-Departmental Public Body or Assembly Sponsored Public Body (advisory, executive, or tribunal);<br>b) Non-Ministerial Department; or<br>c) Executive Agency; |
| **Change in Law** | any change in Law which impacts on the supply of the Deliverables and performance of the Contract which comes into force after the Start Date; |
| **Change of Control** | a change of control within the meaning of Section 450 of the Corporation Tax Act 2010; |
| **Charges** | the prices (exclusive of any applicable VAT), payable to the Supplier by the Buyer under the Call-Off Contract, as set out in the Order Form, for the full and proper performance by the Supplier of its obligations under the Call-Off Contract less any Deductions; |
| **Civil Service Year Books** | means an annual reference guide to the British Civil Service and Non-Departmental Buyer. |

| | |
|---|---|
| **Claim** | any claim which it appears that a Beneficiary is, or may become, entitled to indemnification under this Contract; |
| **Clinic** | means a location or department within a hospital designed for treatment of outpatients. |
| **Closed** | means a Record shall be transferred to The National Archives although withheld from release for a specified time as it is considered to contain Sensitive information which is protected by legal Exemption(s) and whose closure has been approved by the Secretary of State for Culture, Media and Sport on the advice of the Advisory Council on National Records and Archives (ACNRA). |
| **Commercially Sensitive Information** | the Confidential Information listed in the Framework Award Form or Order Form (if any) comprising of commercially sensitive information relating to the Supplier, its IPR or its business or which the Supplier has indicated to the Authority that, if disclosed by the Authority, would cause the Supplier significant commercial disadvantage or material financial loss; |
| **Comparable Supply** | the supply of Deliverables to another Buyer of the Supplier that are the same or similar to the Deliverables; |
| **Compliance Officer** | the person(s) appointed by the Supplier who is responsible for ensuring that the Supplier complies with its legal obligations; |
| **Confidential Information** | means any information, however it is conveyed, that relates to the business, affairs, developments, trade secrets, Know-How, personnel and suppliers of CCS, the Buyer or the Supplier, including IPRs, together with information derived from the above, and any other information clearly designated as being confidential (whether or not it is marked as **"confidential"**) or which ought reasonably to be considered to be confidential; |
| **Conflict of Interest** | a conflict between the financial or personal duties of the Supplier or the Supplier Staff and the duties owed to CCS or any Buyer under a Contract, in the reasonable opinion of the Buyer or CCS; |
| **Consumables** | means goods that need to be replenished in accordance with this Framework Schedule 2. |
| **Contract** | either the Framework Contract or the Call-Off Contract, as the context requires; |
| **Contract Manager** | to Buyers on a minimum of a monthly and quarterly basis detailing any key issues or risks which the Supplier feels the Authority (Framework Contract level) or Buyer's (Call Off Contract level) should be aware of and progress against previously agreed key initiatives and actions. |

| | |
|---|---|
| **Contract Period** | the term of either a Framework Contract or Call-Off Contract on and from the earlier of the:<br>a)applicable Start Date; or<br>b)the Effective Date<br>up to and including the applicable End Date; |
| **Contract Value** | the higher of the actual or expected total Charges paid or payable under a Contract where all obligations are met by the Supplier; |
| **Contract Year** | a consecutive period of twelve (12) Months commencing on the Start Date or each anniversary thereof; |
| **Control** | control in either of the senses defined in sections 450 and 1124 of the Corporation Tax Act 2010 and "**Controlled**" shall be construed accordingly; |
| **Controller** | has the meaning given to it in the GDPR; |
| **Core Terms** | CCS' standard terms and conditions for common goods and services which govern how Supplier must interact with CCS and Buyers under Framework Contracts and Call-Off Contracts; |
| **Costs** | the following costs (without double recovery) to the extent that they are reasonably and properly incurred by the Supplier in providing the Deliverables:<br>e) the cost to the Supplier or the Key Subcontractor (as the context requires), calculated per Work Day, of engaging the Supplier Staff, including:<br>i) base salary paid to the Supplier Staff;<br>ii) employer's National Insurance contributions;<br>iii) pension contributions;<br>iv) car allowances;<br>v) any other contractual employment benefits;<br>vi) staff training;<br>vii) work place accommodation;<br>viii)work place IT equipment and tools reasonably necessary to provide the Deliverables (but not including items included within limb (b) below); and<br>ix) reasonable recruitment costs, as agreed with the Buyer;<br>f) costs incurred in respect of Supplier Assets which would be treated as capital costs according to generally accepted accounting principles within the UK, which shall include the cost to be charged in respect of Supplier Assets by the Supplier to the Buyer or (to the extent that risk and title in any Supplier |

| | |
|---|---|
| | Asset is not held by the Supplier) any cost actually incurred by the Supplier in respect of those Supplier Assets;<br>g) operational costs which are not included within (a) or (b) above, to the extent that such costs are necessary and properly incurred by the Supplier in the provision of the Deliverables; and<br>h) Reimbursable Expenses to the extent these have been specified as allowable in the Order Form and are incurred in delivering any Deliverables;<br>but excluding:<br>i) Overhead;<br>j) financing or similar costs;<br>k) maintenance and support costs to the extent that these relate to maintenance and/or support Deliverables provided beyond the Call-Off Contract Period whether in relation to Supplier Assets or otherwise;<br>l) taxation;<br>m) fines and penalties;<br>n) amounts payable under Call-Off Schedule 16 (Benchmarking) where such Schedule is used; and<br>o) non-cash items (including depreciation, amortisation, impairments and movements in provisions); |
| **CRTPA** | the Contract Rights of Third Parties Act 1999; |
| **Dashboard Report** | means a high level performance report, utilising graphs and charts to indicate trends and variances in performance, covering a period to be specified. |
| **Data** | means Data relating to Records within the Scanning Service (Off and/or On-Site). |
| **Data Protection Impact Assessment** | an assessment by the Controller of the impact of the envisaged Processing on the protection of Personal Data; |
| **Data Protection Legislation** | the GDPR, the LED and any applicable national implementing Laws as amended from time to time (ii) the DPA 2018 to the extent that it relates to Processing of personal data and privacy; (iii) all applicable Law about the Processing of personal data and privacy; |
| **Data Protection Liability Cap** | the amount specified in the Framework Award Form; |
| **Data Protection Officer** | has the meaning given to it in the GDPR; |
| **Data Subject** | has the meaning given to it in the GDPR; |

| | |
|---|---|
| **Data Subject Access Request** | a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to access their Personal Data; |
| **Deductions** | all Service Credits, Delay Payments (if applicable), or any other deduction which the Buyer is paid or is payable to the Buyer under a Call-Off Contract; |
| **Default** | any breach of the obligations of the Supplier (including abandonment of a Contract in breach of its terms) or any other default (including material default), act, omission, negligence or statement of the Supplier, of its Subcontractors or any Supplier Staff howsoever arising in connection with or in relation to the subject-matter of a Contract and in respect of which the Supplier is liable to the Relevant Authority; |
| **Default Management Charge** | has the meaning given to it in Paragraph 8.1.1 of Framework Schedule 5 (Management Charges and Information); |
| **Delay Payments** | the amounts (if any) payable by the Supplier to the Buyer in respect of a delay in respect of a Milestone as specified in the Implementation Plan; |
| **Deliverables** | Goods and/or Services that may be ordered under the Contract including the Documentation; |
| **Delivery** | delivery of the relevant Deliverable or Milestone in accordance with the terms of a Call-Off Contract as confirmed and accepted by the Buyer by the either (a) confirmation in writing to the Supplier; or (b) where Call-Off Schedule 13 (Implementation Plan and Testing) is used issue by the Buyer of a Satisfaction Certificate. "**Deliver**" and "**Delivered**" shall be construed accordingly; |
| **Departmental Appraisal** | means the process of identifying Records containing historical information by reviewing Records as per the Buyer's organisational structure e.g. finance, HR and policy departments |
| **Departmental Records Officer** | means the Buyer's representative who is responsible for all information the organisation creates and holds, and understands the value of that information from a business and legal perspective |
| **Deputy Framework Manager** | means the person(s) who deputises for the Framework Manager |
| **Destruction** | means the final stage whereby a Record which is no longer worthwhile or needed in terms of administrations, research or law is sorted and disposed of in accordance with set procedures. |

| | |
|---|---|
| **Destruction Certificate** | means the documentation which the Supplier is required to produce to accompany all Destructions (Physical or electronic, single Destruction or Bulk Destruction) of Buyers Records. |
| **Destruction Date** | means the day, the month or the year upon which a Record which is no longer worthwhile or needed in terms of administrations, research or law is sorted and disposed of in accordance with set procedures. |
| **Digital/ Digitising** | (Records) means the process to convert a Records into a digital format enabling it to be processed by a computer. |
| **Dip Sample** | means a selection of a random sample of Records |
| **Disclosure and Barring Service (DBS)** | means the Disclosure and Barring Service (DBS) which is a non departmental authority of the Home Office of the United Kingdom. |
| **Disclosing Party** | the Party directly or indirectly providing Confidential Information to the other Party in accordance with Clause 15 (What you must keep confidential); |
| **Disposal** | means the point in a Records lifecycle when they are either transferred to an archive or destroyed and is undertaken in accordance with clearly established policies which have been formerly adopted by Buyers. |
| **Dispute** | any claim, dispute or difference (whether contractual or non-contractual) arising out of or in connection with the Contract or in connection with the negotiation, existence, legal validity, enforceability or termination of the Contract, whether the alleged liability shall arise under English law or under the law of some other country and regardless of whether a particular cause of action may successfully be brought in the English courts; |
| **Dispute Resolution Procedure** | the dispute resolution procedure set out in Clause 34 (Resolving disputes); |
| **Documents Repository System (DRS)** | means the system utilised by Buyers and the Supplier to store and electronically re-call scanned records. The DRS stores and manages scanned Images, Records and other types of documents. |
| **Document Storage Solution Development** | means the process of constituting a new stage or a change in situation for a space which is devoted to the overflow storage of document files in any media |
| **Documentation** | descriptions of the Services and Service Levels, technical specifications, user manuals, training manuals, operating manuals, process definitions and procedures, system environment descriptions and all such other documentation (whether in hardcopy |

| | |
|---|---|
| | or electronic form) is required to be supplied by the Supplier to the Buyer under a Contract as:<br>a) would reasonably be required by a competent third party capable of Good Industry Practice contracted by the Buyer to develop, configure, build, deploy, run, maintain, upgrade and test the individual systems that provide the Deliverables<br>b) is required by the Supplier in order to provide the Deliverables; and/or<br>c) has been or shall be generated for the purpose of providing the Deliverables; |
| **DOTAS** | the Disclosure of Tax Avoidance Schemes rules which require a promoter of tax schemes to tell HMRC of any specified notifiable arrangements or proposals and to provide prescribed information on those arrangements or proposals within set time limits as contained in Part 7 of the Finance Act 2004 and in secondary legislation made under vires contained in Part 7 of the Finance Act 2004 and as extended to National Insurance Contributions; |
| **DPA 2018** | the Data Protection Act 2018; |
| **Due Diligence Information** | any information supplied to the Supplier by or on behalf of the Authority prior to the Start Date; |
| **Effective Date** | the date on which the final Party has signed the Contract; |
| **EIR** | the Environmental Information Regulations 2004; |
| **Electronic Invoice** | an invoice which has been issued, transmitted and received in a structured electronic format which allows for its automatic and electronic processing and which complies with (a) the European standard and (b) any of the syntaxes published in Commission Implementing Decision (EU) 2017/1870; |
| **Electronic Retrieval** | means the activity of electronically obtaining information resources relevant to an information need End to End means the full lifecycle of Scanning Services, from intake to Destruction activity and any residual activity resulting from the Records destruction. |
| **Employment Regulations** | the Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) as amended or replaced or any other Regulations implementing the European Council Directive 77/187/EEC; |
| **End Date** | the earlier of:<br>a) the Expiry Date (as extended by any Extension Period exercised by the Relevant Authority under Clause 10.1.2); or<br>b) if a Contract is terminated before the date specified in (a) above, the date of termination of the Contract; |

| | |
|---|---|
| **End to End** | means the full lifecycle of Scanning Services, from intake to Destruction activity and any residual activity resulting from the Records destruction. |
| **Entry Strategy** | means Supplier's plan to manage the Intake of the Buyer's Records and/or Boxes in line with requirements stated at Call Off stage. |
| **Environmental Policy** | to conserve energy, water, wood, paper and other resources, reduce waste and phase out the use of ozone depleting substances and minimise the release of greenhouse gases, volatile organic compounds and other substances damaging to health and the environment, including any written environmental policy of the Buyer; |
| **Equality and Human Rights Commission** | the UK Government body named as such as may be renamed or replaced by an equivalent body from time to time; |
| **Equipment** | means the Equipment required by the Supplier to undertake the Services it has been contracted to perform. |
| **Estimated Year 1 Charges** | the anticipated total Charges payable by the Buyer in the first Contract Year specified in the Order Form; |

**Estimated Yearly Charges**

means for the purposes of calculating each Party's annual liability under clause 11.2:

i) in the first Contract Year, the Estimated Year 1 Charges; or

ii) in the any subsequent Contract Years, the Charges paid or payable in the previous Call-off Contract Year; or

iii) after the end of the Call-off Contract, the Charges paid or payable in the last Contract Year during the Call-off Contract Period;

| | |
|---|---|
| **Exempt Buyer** | a public sector purchaser that is:<br>a) eligible to use the Framework Contract; and<br>) is entering into an Exempt Call-off Contract that is not subject to (as applicable) any of:<br>i) the Regulations;<br>ii) the Concession Contracts Regulations 2016 (SI 2016/273);<br>iii) the Utilities Contracts Regulations 2016 (SI 2016/274); |

iv) the Defence and Security Public Contracts Regulations 2011 (SI 2011/1848);

v) the Remedies Directive (2007/66/EC);

vi) Directive 2014/23/EU of the European Parliament and Council;

vii) Directive 2014/24/EU of the European Parliament and Council;

viii) Directive 2014/25/EU of the European Parliament and Council; or

ix) Directive 2009/81/EC of the European Parliament and Council;

| | |
|---|---|
| **Exempt Call-off Contract** | the contract between the Exempt Buyer and the Supplier for Deliverables which consists of the terms set out and referred to in the Order Form incorporating and, where necessary, amending, refining or adding to the terms of the Framework Contract; |
| **Exempt Procurement Amendments** | any amendments, refinements or additions to any of the terms of the Framework Contract made through the Exempt Call-off Contract to reflect the specific needs of an Exempt Buyer to the extent permitted by and in accordance with any legal requirements applicable to that Exempt Buyer; |

| | |
|---|---|
| **Exemptions** | means the reasons to withhold information |
| **Existing IPR** | any and all IPR that are owned by or licensed to either Party and which are or have been developed independently of the Contract (whether prior to the Start Date or otherwise); |
| **Exit Day** | shall have the meaning in the European Union (Withdrawal) Act 2018; |
| **Exit Strategy** | means Supplier's plan to manage the Permanent Withdrawal or all Records and/or Boxes in line with Call Off Agreement agreed which shall include timeline and costs. |
| **Expiry Date** | the Framework Expiry Date or the Call-Off Expiry Date (as the context dictates); |
| **Extension Period** | the Framework Optional Extension Period or the Call-Off Optional Extension Period as the context dictates; |

| | |
|---|---|
| **FOIA** | the Freedom of Information Act 2000 and any subordinate legislation made under that Act from time to time together with any guidance and/or codes of practice issued by the Information Commissioner or relevant Government department in relation to such legislation; |
| **Force Majeure Event** | any event, occurrence, circumstance, matter or cause affecting the performance by either the Relevant Authority or the Supplier of its obligations arising from acts, events, omissions, happenings or non-happenings beyond the reasonable control of the Affected Party which prevent or materially delay the Affected Party from performing its obligations under a Contract and which are not attributable to any wilful act, neglect or failure to take reasonable preventative action by the Affected Party, including:<br>a) riots, civil commotion, war or armed conflict;<br>b) acts of terrorism;<br>c) acts of a Central Government Body, local government or regulatory bodies;<br>d) fire, flood, storm or earthquake or other natural disaster,<br>but excluding any industrial dispute relating to the Supplier, the Supplier Staff or any other failure in the Supplier or the Subcontractor's supply chain; |
| **Force Majeure Notice** | a written notice served by the Affected Party on the other Party stating that the Affected Party believes that there is a Force Majeure Event; |
| **Framework** | means this agreement consisting of the core terms and all associated schedules |
| **Framework Award Form** | the document outlining the Framework Incorporated Terms and crucial information required for the Framework Contract, to be executed by the Supplier and CCS; |
| **Framework Contract** | the framework established between CCS and the Supplier in accordance with Regulation 33 by the Framework Award Form for the provision of the Deliverables to Buyers by the Supplier pursuant to the OJEU Notice; |
| **Framework Contract Period** | the period from the Framework Start Date until the End Date of the Framework Contract; |
| **Framework Expiry Date** | the scheduled date of the end of the Framework Contract as stated in the Framework Award Form; |

| | |
|---|---|
| **Framework Incorporated Terms** | the contractual terms applicable to the Framework Contract specified in the Framework Award Form; |
| **Framework Manager** | means the person(s) who is suitably experienced and who is responsible for ensuring that all the requirements of the Framework Agreement are met or exceeded and must be familiar with all aspects of the Framework Agreement. |
| **Framework Optional Extension Period** | such period or periods beyond which the Framework Contract Period may be extended as specified in the Framework Award Form; |
| **Framework Price(s)** | the price(s) applicable to the provision of the Deliverables set out in Framework Schedule 3 (Framework Prices); |
| **Framework Special Terms** | any additional terms and conditions specified in the Framework Award Form incorporated into the Framework Contract; |
| **Framework Start Date** | the date of start of the Framework Contract as stated in the Framework Award Form; |
| **Framework Tender Response** | the tender submitted by the Supplier to CCS and annexed to or referred to in Framework Schedule 2 (Framework Tender); |
| **Further Competition Procedure** | the further competition procedure described in Framework Schedule 7 (Call-Off Award Procedure); |
| **GDPR** | the General Data Protection Regulation (Regulation (EU) 2016/679); |
| **General Anti-Abuse Rule** | e)the legislation in Part 5 of the Finance Act 2013 and; and<br>c) any future legislation introduced into parliament to counteract tax advantages arising from abusive arrangements to avoid National Insurance contributions; |
| **General Change in Law** | a Change in Law where the change is of a general legislative nature (including taxation or duties of any sort affecting the Supplier) or which affects or relates to a Comparable Supply; |
| **Goods** | goods made available by the Supplier as specified in Framework Schedule 1 (Specification) and in relation to a Call-Off Contract as specified in the Order Form ; |
| **Good Industry Practice** | standards, practices, methods and procedures conforming to the Law and the exercise of the degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person or body engaged within the relevant industry or business sector; |

| | |
|---|---|
| **Government** | the government of the United Kingdom (including the Northern Ireland Assembly and Executive Committee, the Scottish Government and the National Assembly for Wales), including government ministers and government departments and other bodies, persons, commissions or agencies from time to time carrying out functions on its behalf; |
| **Government Buying Standards (GBS)** | means the set of standards the Government buyers must follow and the information about sustainable procurement and how it should be applied when buying goods and services. |
| **Government Data** | the data, text, drawings, diagrams, images or sounds (together with any database made up of any of these) which are embodied in any electronic, magnetic, optical or tangible media, including any of the Authority's Confidential Information, and which:<br>i) are supplied to the Supplier by or on behalf of the Authority; or<br>ii) the Supplier is required to generate, process, store or transmit pursuant to a Contract; |
| **Government Security Classification Policy** | means the system for classifying sensitive government Data in the United Kingdom. |
| **Government Social Values** | means the way the Government buyers applies it's thought processes around how scarce resources are allocated and used. It involves looking beyond the price of each individual Contract and looking at what the collective benefit to a community is when Buyers choose to award a Contract. |
| **Guarantor** | the person (if any) who has entered into a guarantee in the form set out in Joint Schedule 8 (Guarantee) in relation to this Contract; |
| **Halifax Abuse Principle** | the principle explained in the CJEU Case C-255/02 Halifax and others; |
| **High Level Appraisal Methodology** | means the methodology defined by the Buyer in order to undertake a High Level Appraisal of its Records |
| **Highlight Report** | means a report which is sent by the Supplier's Framework Manager and Call Off |
| **HMRC** | Her Majesty's Revenue and Customs; |
| **ICT Policy** | the Buyer's policy in respect of information and communications technology, referred to in the Order Form, which is in force as at the |

| | |
|---|---|
| | Call-Off Start Date (a copy of which has been supplied to the Supplier), as updated from time to time in accordance with the Variation Procedure; |
| **Impact Assessment** | an assessment of the impact of a Variation request by the Relevant Authority completed in good faith, including:<br>a) details of the impact of the proposed Variation on the Deliverables and the Supplier's ability to meet its other obligations under the Contract;<br>b) details of the cost of implementing the proposed Variation;<br>c) details of the ongoing costs required by the proposed Variation when implemented, including any increase or decrease in the Framework Prices/Charges (as applicable), any alteration in the resources and/or expenditure required by either Party and any alteration to the working practices of either Party;<br>d) a timetable for the implementation, together with any proposals for the testing of the Variation; and<br>e) such other information as the Relevant Authority may reasonably request in (or in response to) the Variation request; |
| **Implementation Plan** | the plan for provision of the Deliverables set out in Call-Off Schedule 13 (Implementation Plan and Testing) where that Schedule is used or otherwise as agreed between the Supplier and the Buyer; |
| **Implementation Plan (IP)** | means a plan which is to be agreed between Buyers and Supplier after Contract Award, detailing the plan to implement the new service provision while also detailing actions, deliverables and timescales. |
| **Implementation Period** | means the period of time agreed to implement the Contract and/or Service prior to Contract commencement date. |
| **Inactive Records** | means a Record which is no longer referenced on a regular basis, but must be kept for administrative, historical or legal purposes and is therefore stored in a less accessible place since it is not used frequently. |
| **Indemnifier** | a Party from whom an indemnity is sought under this Contract; |
| **Independent Control** | where a Controller has provided Personal Data to another Party which is not a Processor or a Joint Controller because the recipient itself determines the purposes and means of Processing but does so separately from the Controller providing it with Personal Data and "**Independent Controller**" shall be construed accordingly; |

| | |
|---|---|
| **Indexation** | the adjustment of an amount or sum in accordance with Framework Schedule 3 (Framework Prices) and the relevant Order Form; |
| **Induction** | Means an event attended by the Buyer and Supplier. The purpose of the event is for the Buyer to share details of the information sources required to be utilised by the Supplier in order to conduct the services on behalf of the Buyer. |
| **Information** | has the meaning given under section 84 of the Freedom of Information Act 2000; |
| **Information Commissioner** | the UK's independent authority which deals with ensuring information relating to rights in the public interest and data privacy for individuals is met, whilst promoting openness by public bodies; |
| **Initial Period** | the initial term of a Contract specified in the Framework Award Form or the Order Form, as the context requires; |
| **Insolvency Event** | with respect to any person, means:<br>(a) that person suspends, or threatens to suspend, payment of its debts, or is unable to pay its debts as they fall due or admits inability to pay its debts, or:<br>(i) (being a company or a LLP) is deemed unable to pay its debts within the meaning of section 123 of the Insolvency Act 1986, or<br>(ii) (being a partnership) is deemed unable to pay its debts within the meaning of section 222 of the Insolvency Act 1986;<br>(b) that person commences negotiations with one or more of its creditors (using a voluntary arrangement, scheme of arrangement or otherwise) with a view to rescheduling any of its debts, or makes a proposal for or enters into any compromise or arrangement with one or more of its creditors or takes any step to obtain a moratorium pursuant to Section 1A and Schedule A1 of the Insolvency Act 1986 other than (in the case of a company, a LLP or a partnership) for the sole purpose of a scheme for a solvent amalgamation of that person with one or more other companies or the solvent reconstruction of that person;<br>(c) another person becomes entitled to appoint a receiver over the assets of that person or a receiver is appointed over the assets of that person;<br>(d) a creditor or encumbrancer of that person attaches or takes possession of, or a distress, execution or other such process is levied or enforced on or sued against, the whole or any part of that person's assets and such attachment or process is not discharged within 14 days; |

| | |
|---|---|
| | (e) that person suspends or ceases, or threatens to suspend or cease, carrying on all or a substantial part of its business;<br><br>(f) where that person is a company, a LLP or a partnership:<br><br>(i) a petition is presented (which is not dismissed within 14 days of its service), a notice is given, a resolution is passed, or an order is made, for or in connection with the winding up of that person other than for the sole purpose of a scheme for a solvent amalgamation of that person with one or more other companies or the solvent reconstruction of that person;<br><br>(ii) an application is made to court, or an order is made, for the appointment of an administrator, or if a notice of intention to appoint an administrator is filed at Court or given or if an administrator is appointed, over that person;<br><br>(iii) (being a company or a LLP) the holder of a qualifying floating charge over the assets of that person has become entitled to appoint or has appointed an administrative receiver; or<br><br>(iv) (being a partnership) the holder of an agricultural floating charge over the assets of that person has become entitled to appoint or has appointed an agricultural receiver; or<br><br>(g) any event occurs, or proceeding is taken, with respect to that person in any jurisdiction to which it is subject that has an effect equivalent or similar to any of the events mentioned above; |
| **Installation Works** | all works which the Supplier is to carry out at the beginning of the Call-Off Contract Period to install the Goods in accordance with the Call-Off Contract; |
| **Intellectual Property Rights or IPR** | a) copyright, rights related to or affording protection similar to copyright, rights in databases, patents and rights in inventions, semi-conductor topography rights, trade marks, rights in internet domain names and website addresses and other rights in trade or business names, goodwill, designs, Know-How, trade secrets and other rights in Confidential Information;<br>b) applications for registration, and the right to apply for registration, for any of the rights listed at (a) that are capable of being registered in any country or jurisdiction; and<br>c) all other rights having equivalent or similar effect in any country or jurisdiction; |
| **Internal Workflow** | Means a sequence of processes through which a piece of work or a document passes from initiation to completion. |

| | |
|---|---|
| **Inventory Management** | means a list and or report detailing the description and or movement of a Record. |
| **Inventory Software** | means a computer-based system for tracking inventory levels, orders and movements of goods |
| **Invoicing Address** | the address to which the Supplier shall invoice the Buyer as specified in the Order Form; |
| **IPR Claim** | any claim of infringement or alleged infringement (including the defence of such infringement or alleged infringement) of any IPR, used to provide the Deliverables or otherwise provided and/or licensed by the Supplier (or to which the Supplier has provided access) to the Relevant Authority in the fulfilment of its obligations under a Contract; |
| **IR35** | the off-payroll rules requiring individuals who work through their company pay the same tax and National Insurance contributions as an employee which can be found online at: https://www.gov.uk/guidance/ir35-find-out-if-it-applies; |
| **Joint Controller Agreement** | the agreement (if any) entered into between the Relevant Authority and the Supplier substantially in the form set out in Annex 2 of Joint Schedule 11 (*Processing Data*); |
| **Joint Controllers** | where two or more Controllers jointly determine the purposes and means of Processing; |
| **Key Staff** | the individuals (if any) identified as such in the Order Form; |
| **Key Sub-Contract** | each Sub-Contract with a Key Subcontractor; |
| **Key Subcontractor** | any Subcontractor:<br>a) which is relied upon to deliver any work package within the Deliverables in their entirety; and/or<br>b) which, in the opinion of CCS or the Buyer performs (or would perform if appointed) a critical role in the provision of all or any part of the Deliverables; and/or<br>c) with a Sub-Contract with a contract value which at the time of appointment exceeds (or would exceed if appointed) 10% of the aggregate Charges forecast to be payable under the Call-Off Contract,<br>and the Supplier shall list all such Key Subcontractors in section 19 of the Framework Award Form and in the Key Subcontractor Section in Order Form; |

| | |
|---|---|
| **Know-How** | all ideas, concepts, schemes, information, knowledge, techniques, methodology, and anything else in the nature of know-how relating to the Deliverables but excluding know-how already in the other Party's possession before the applicable Start Date; |
| **Law** | any law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, enforceable right within the meaning of Section 2 of the European Communities Act 1972, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements with which the relevant Party is bound to comply; |
| **LED** | Law Enforcement Directive (Directive (EU) 2016/680); |
| **Lister** | means the Supplier Personnel who will transcribe and input information from a Record into a list. |
| **Lister Project Manager** | means the Project Manager who oversees the Lister and Lister Service. |
| **Listing Service** | means the process of transcribing and inputting information from a Record into a list which shall then be transposed into a Catalogue template |
| **Loose Filing** | means when a Patient's Record is not available during the Patient's appointment therefore a temporary Record is compiled and then subsequently enclosed within the original Patient Record. |
| **Losses** | all losses, liabilities, damages, costs, expenses (including legal fees), disbursements, costs of investigation, litigation, settlement, judgment, interest and penalties whether arising in contract, tort (including negligence), breach of statutory duty, misrepresentation or otherwise and "**Loss**" shall be interpreted accordingly; |
| **Lots** | the number of lots specified in Framework Schedule 1 (Specification), if applicable; |
| **Macro level Appraisal** | means a process within a Buyers business function(s) between a certain time period, in order to identify information of historical importance and determine whether further appraisal techniques shall be undertaken. |
| **Management Charge** | the sum specified in the Framework Award Form payable by the Supplier to CCS in accordance with Framework Schedule 5 (Management Charges and Information); |
| **Management Information or MI** | the management information specified in Framework Schedule 5 (Management Charges and Information); |

| | |
|---|---|
| **Marketing and Communications Plan** | means the plan agreed between the Authority and the Supplier which will detail all marketing activities including, but not limited to, producing case studies, running or attending events, direct mail campaigns, and Social Media campaigns. |
| **Material** | means wording, photographs, Images, maps or any content within the Record(s). |
| **Microfiche means** | a flat piece of film containing microphotographs of the pages of a newspaper, catalogue, or other document. |
| **Microfilm** | means film containing microphotographs of a newspaper, catalogue, or other document. |
| **Microform** | means microphotographic reproduction, on film or paper, of a manuscript, map, or other document. |
| **Milestone** | an event or task described in the Implementation Plan; |
| **Milestone Date** | the target date set out against the relevant Milestone in the Implementation Plan by which the Milestone must be Achieved; |
| **Mixed Appraisal** | means the undertaking of a mixture of appraisal processes in order to identify information of historical importance |
| **MI Default** | means when two (2) MI Reports are not provided in any rolling six (6) month period |
| **MI Failure** | means when an MI report:<br>a) contains any material errors or material omissions or a missing mandatory field; or<br>b) is submitted using an incorrect MI reporting Template; or<br>c) is not submitted by the reporting date (including where a declaration of no business should have been filed); |
| **MI Report** | means a report containing Management Information submitted to the Authority in accordance with Framework Schedule 5 (Management Charges and Information); |
| **MI Reporting Template** | means the form of report set out in the Annex to Framework Schedule 5 (Management Charges and Information) setting out the information the Supplier is required to supply to the Authority; |
| **Month** | a calendar month and "**Monthly**" shall be interpreted accordingly; |
| **National Cyber Security Centre (NCSC)** | Means an organisation within the UK Government that provides advice and support for the public and private sector in how to avoid computer threats. |

| | |
|---|---|
| **National Insurance** | contributions required by the Social Security Contributions and Benefits Act 1992 and made in accordance with the Social Security (Contributions) Regulations 2001 (SI 2001/1004); |
| **New IPR** | IPR in items created by the Supplier (or by a third party on behalf of the Supplier) specifically for the purposes of a Contract and updates and amendments of these items including (but not limited to) database schema; and/or<br><br>IPR in or arising as a result of the performance of the Supplier's obligations under a Contract and all updates and amendments to the same;<br><br>but shall not include the Supplier's Existing IPR; |
| **Occasion of Tax Non–Compliance** | where:<br><br>a) any tax return of the Supplier submitted to a Relevant Tax Authority on or after 1 October 2012 which is found on or after 1 April 2013 to be incorrect as a result of:<br><br>i) a Relevant Tax Authority successfully challenging the Supplier under the General Anti-Abuse Rule or the Halifax Abuse Principle or under any tax rules or legislation in any jurisdiction that have an effect equivalent or similar to the General Anti-Abuse Rule or the Halifax Abuse Principle;<br><br>ii) the failure of an avoidance scheme which the Supplier was involved in, and which was, or should have been, notified to a Relevant Tax Authority under the DOTAS or any equivalent or similar regime in any jurisdiction; and/or<br><br>b) any tax return of the Supplier submitted to a Relevant Tax Authority on or after 1 October 2012 which gives rise, on or after 1 April 2013, to a criminal conviction in any jurisdiction for tax related offences which is not spent at the Start Date or to a civil penalty for fraud or evasion; |
| **Off-site Sensitivity Review Service** | means the Supplier who shall conduct a Sensitivity Review of Record(s) at the Suppliers premises. |
| **On-site** | means the Services performed at a designated Buyers office or other location |
| **On-site Sensitivity Review Service** | means the Supplier who shall conduct the Sensitivity Review of Record(s) at the Buyers premises. |
| **On Premise** | means software supplied, installed and ran on hardware and/or systems on the premises of the Buyer using the software. |
| **Off Premise** | means software supplied and managed |

| | |
|---|---|
| **Open** | means the Record does not contain Sensitive information and therefore shall be transferred to The National Archives and Open to the public. |
| **Open Book Data** | complete and accurate financial and non-financial information which is sufficient to enable the Buyer to verify the Charges already paid or payable and Charges forecast to be paid during the remainder of the Call-Off Contract, including details and all assumptions relating to:<br>a) the Supplier's Costs broken down against each Good and/or Service and/or Deliverable, including actual capital expenditure (including capital replacement costs) and the unit cost and total actual costs of all Deliverables;<br>b) operating expenditure relating to the provision of the Deliverables including an analysis showing:<br>iii) the unit costs and quantity of Goods and any other consumables and bought-in Deliverables;<br>iv) staff costs broken down into the number and grade/role of all Supplier Staff (free of any contingency) together with a list of agreed rates against each grade;<br>v) a list of Costs underpinning those rates for each grade, being the agreed rate less the Supplier Profit Margin; and<br>iii) Reimbursable Expenses, if allowed under the Order Form;<br>c) Overheads;<br>d) all interest, expenses and any other third party financing costs incurred in relation to the provision of the Deliverables;<br>e) the Supplier Profit achieved over the Framework Contract Period and on an annual basis;<br>f) confirmation that all methods of Cost apportionment and Overhead allocation are consistent with and not more onerous than such methods applied generally by the Supplier;<br>g) an explanation of the type and value of risk and contingencies associated with the provision of the Deliverables, including the amount of money attributed to each risk and/or contingency; and<br>h) the actual Costs profile for each Service Period; |
| **Order** | means an order for the provision of the Deliverables placed by a Buyer with the Supplier under a Contract; |
| **Order Form** | a completed Order Form Template (or equivalent information issued by the Buyer) used to create a Call-Off Contract; |

| | |
|---|---|
| **Order Form Template** | the template in Framework Schedule 6 (Order Form Template and Call-Off Schedules); |
| **Other Contracting Authority** | any actual or potential Buyer under the Framework Contract; |
| **Overhead** | those amounts which are intended to recover a proportion of the Supplier's or the Key Subcontractor's (as the context requires) indirect corporate costs (including financing, marketing, advertising, research and development and insurance costs and any fines or penalties) but excluding allowable indirect costs apportioned to facilities and administration in the provision of Supplier Staff and accordingly included within limb (a) of the definition of "Costs"; |
| **Page-by-Page review** | means the process of identifying information of historical importance within the Record by reviewing pages within the Record. |
| **Parliament** | takes its natural meaning as interpreted by Law; |
| **Partially Closed** | means a Record which has been released to the public, although part of that Record has been withheld from release as it is considered to contain Sensitive information which is protected by legal Exemption(s) and whose closure has been approved by the Secretary of State for Culture, Media and Sport on the advice of the Advisory Council on National Records and Archives (ACNRA). |
| **Party** | in the context of the Framework Contract, CCS or the Supplier, and in the in the context of a Call-Off Contract the Buyer or the Supplier. "**Parties**" shall mean both of them where the context permits; |
| **Performance Improvement Plan** | means a plan that recognises failures in delivery and identifies corrective action(s) and timeline(s) for each targeted performance are with assigned accountability. |
| **Performance Indicators or PIs** | the performance measurements and targets in respect of the Supplier's performance of the Framework Contract set out in Framework Schedule 4 (Framework Management); |
| **Permanent Preservation** | means Records that contain information of historical importance that shall be permanently preserved at The National Archives or Place of Deposit |
| **Permanently Withdrawn** | means Records that the Buyer requires to be withdrawn from store permanently and not be returned into store at any point. |
| **Personal Data** | has the meaning given to it in the GDPR; |
| **"Personal Data Breach"** | has the meaning given to it in the GDPR; |

| | |
|---|---|
| **Personnel** | all directors, officers, employees, agents, consultants and suppliers of a Party and/or of any Subcontractor and/or Subprocessor engaged in the performance of its obligations under a Contract; |
| **Physical (Records)** | means any Buyers Record(s), supporting post or Box. |
| **Place of Deposit** | means an appointed repository which holds certain classes of public Records which are not held at The National Archives |
| **Prescribed Person** | a legal adviser, an MP or an appropriate body which a whistle-blower may make a disclosure to as detailed in 'Whistleblowing: list of prescribed people and bodies', 24 November 2016, available online at: https://www.gov.uk/government/publications/blowing-the-whistle-list-of-prescribed-people-and-bodies--2/whistleblowing-list-of-prescribed-people-and-bodies; |
| **Processing** | has the meaning given to it in the GDPR; |
| **Processor** | has the meaning given to it in the GDPR; |
| **Processor Personnel** | all directors, officers, employees, agents, consultants and suppliers of the Processor and/or of any Subprocessor engaged in the performance of its obligations under a Contract; |
| **Product Range** | means the range of New Equipment and Software, together with all associated and specified requirements that will be available to Buyers via this Framework Agreement. |
| **Progress Meeting** | a meeting between the Buyer Authorised Representative and the Supplier Authorised Representative; |
| **Progress Meeting Frequency** | the frequency at which the Supplier shall conduct a Progress Meeting in accordance with Clause 6.1 as specified in the Order Form; |
| **Progress Report** | a report provided by the Supplier indicating the steps taken to achieve Milestones or delivery dates; |
| **Progress Report Frequency** | the frequency at which the Supplier shall deliver Progress Reports in accordance with Clause 6.1 as specified in the Order Form; |
| **Prohibited Acts** | a) to directly or indirectly offer, promise or give any person working for or engaged by a Buyer or any other public body a financial or other advantage to:<br>vii) induce that person to perform improperly a relevant function or activity; or<br>viii)reward that person for improper performance of a relevant function or activity;<br>b) to directly or indirectly request, agree to receive or accept any financial or other advantage as an inducement or a reward for |

| | |
|---|---|
| | improper performance of a relevant function or activity in connection with each Contract; or<br>c) committing any offence:<br>ix) under the Bribery Act 2010 (or any legislation repealed or revoked by such Act); or<br>x) under legislation or common law concerning fraudulent acts; or<br>xi) defrauding, attempting to defraud or conspiring to defraud a Buyer or other public body; or<br>d) any activity, practice or conduct which would constitute one of the offences listed under (c) above if such activity, practice or conduct had been carried out in the UK; |
| **Project Manager** | means the person in overall charge of the planning and execution of a particular project. |
| **Protective Measures** | appropriate technical and organisational measures which may include: pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the such measures adopted by it including those outlined in Framework Schedule 9 (Cyber Essentials Scheme), if applicable, in the case of the Framework Contract or Call-Off Schedule 9 (Security), if applicable, in the case of a Call-Off Contract. |
| **Real Time (RT)** | means systems that update information at the same rate as they receive Data. |
| **Recall** | a request by the Supplier to return Goods to the Supplier or the manufacturer after the discovery of safety issues or defects (including defects in the right IPR rights) that might endanger health or hinder performance; |
| **Recipient Party** | the Party which receives or obtains directly or indirectly Confidential Information; |
| **Rectification Plan** | a) the Supplier's plan (or revised plan) to rectify it's breach using the template in Joint Schedule 10 (Rectification Plan) which shall include:<br>b) full details of the Default that has occurred, including a root cause analysis;<br>c) the actual or anticipated effect of the Default; and |

| | |
|---|---|
| | d) the steps which the Supplier proposes to take to rectify the Default (if applicable) and to prevent such Default from recurring, including timescales for such steps and for the rectification of the Default (where applicable); |
| **Rectification Plan Process** | the process set out in Clause 10.3.1 to 10.3.4 (Rectification Plan Process); |
| **Record-by-Record** | Means the Supplier undertaking an Appraisal of Records and reviewing them by each individual Record. |
| **Record(s) Closure Date** | means the date by which information shall remain closed until the Record is re-reviewed. |
| **Record(s)** | means any Buyers' Record, Document, Item, i.e. recorded information, in any form, created or received and maintained by Buyers in the transaction of its business or conduct of affairs and kept as evidence of such activity which is to be stored in the store as part of this Framework Agreement and subsequent Call Off Contracts. |
| **Records Information Management** | means the efficient and systematic control of the creation, receipt, maintenance, use and disposition of Records, including the processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records. |
| **Records Information Management (RIM) System** | means the efficient and systematic control of the creation, receipt, maintenance, use and disposition of Records, including the processes for capturing and maintaining evidence of and information about business activities and transactions in the form of Records. |
| **Record-Level Appraisal** | means undertaking an appraisal of Records at Record Title level within the Contracting Authorities business function at a certain time period to identify information of historical importance. |
| **Record Preparation Service** | means the process conducting the careful Physical preparation of a Record to ensure it remains intact and useable for a specified time period. |
| **Record Preparer** | means Supplier Personnel which shall conduct the process of preparing a Record to ensure that it remains intact and useable for a specified time period. |
| **Record Preparer Project Manager** | means the Project Manager who oversees the Record Preparer and Record Preparation Service |

| | |
|---|---|
| **Record Title Appraisal** | means the process undertaken in order to identify information of historic importance from the name of the Buyer's Record. |
| **Redact (Redacted**) | means the separation of disclosable and non-disclosable information by blocking out individual words, sentences, paragraphs or removal of whole pages or sections prior to release of a document. |
| **Regulations** | the Public Contracts Regulations 2015 and/or the Public Contracts (Scotland) Regulations 2015 (as the context requires); |
| **Reimbursable Expenses** | the reasonable out of pocket travel and subsistence (for example, hotel and food) expenses, properly and necessarily incurred in the performance of the Services, calculated at the rates and in accordance with the Buyer's expenses policy current from time to time, but not including:<br>travel expenses incurred as a result of Supplier Staff travelling to and from their usual place of work, or to and from the premises at which the Services are principally to be performed, unless the Buyer otherwise agrees in advance in writing; and<br>subsistence expenses incurred by Supplier Staff whilst performing the Services at their usual place of work, or to and from the premises at which the Services are principally to be performed; |
| **Relevant Authority** | the Authority which is party to the Contract to which a right or obligation is owed, as the context requires; |
| **Relevant Authority's Confidential Information** | a) all Personal Data and any information, however it is conveyed, that relates to the business, affairs, developments, property rights, trade secrets, Know-How and IPR of the Relevant Authority (including all Relevant Authority Existing IPR and New IPR);<br>b) any other information clearly designated as being confidential (whether or not it is marked "confidential") or which ought reasonably be considered confidential which comes (or has come) to the Relevant Authority's attention or into the Relevant Authority's possession in connection with a Contract; and<br>information derived from any of the above; |
| **Relevant Requirements** | all applicable Law relating to bribery, corruption and fraud, including the Bribery Act 2010 and any guidance issued by the Secretary of State pursuant to section 9 of the Bribery Act 2010; |

| | |
|---|---|
| **Relevant Tax Authority** | HMRC, or, if applicable, the tax authority in the jurisdiction in which the Supplier is established; |
| **Reminder Notice** | a notice sent in accordance with Clause 10.5 given by the Supplier to the Buyer providing notification that payment has not been received on time; |
| **Replacement Deliverables** | any deliverables which are substantially similar to any of the Deliverables and which the Buyer receives in substitution for any of the Deliverables following the Call-Off Expiry Date, whether those goods are provided by the Buyer internally and/or by any third party; |
| **Replacement Subcontractor** | a Subcontractor of the Replacement Supplier to whom Transferring Supplier Employees will transfer on a Service Transfer Date (or any Subcontractor of any such Subcontractor); |
| **"Replacement Supplier"** | any third party provider of Replacement Deliverables appointed by or at the direction of the Buyer from time to time or where the Buyer is providing Replacement Deliverables for its own account, shall also include the Buyer; |
| **Request For Information** | a request for information or an apparent request relating to a Contract for the provision of the Deliverables or an apparent request for such information under the FOIA or the EIRs; |
| **Required Insurances** | the insurances required by Joint Schedule 3 (Insurance Requirements) or any additional insurances specified in the Order Form; |
| **Redact (Redacted)** | means the separation of disclosable and non-disclosable information by blocking out individual words, sentences, paragraphs or removal of whole pages or sections prior to release of a document. |
| **Retained** | means information deemed by Buyers as too sensitive for transfer to The National Archives and will remain with Buyers following approval ACNRA. |
| **Retention Status** | means the status for which the Record(s) have been determined. |
| **Review Date** | means a date which Buyers has stipulated as the date at which the review will take place. |
| **Requestor** | means the User who requests access to the Records Scanning means the process by which paper documents are copied and saved as digital images. |
| **Scanning Services** | means the process by which paper documents are copied and saved as digital images. |

| | |
|---|---|
| **Satisfaction Certificate** | the certificate (materially in the form of the document contained in of Part B of Call-Off Schedule 13 (Implementation Plan and Testing) or as agreed by the Parties where Call-Off Schedule 13 is not used in this Contract) granted by the Buyer when the Supplier has met all of the requirements of an Order, Achieved a Milestone or a Test; |
| **Secure Shredding** | means the process used to cut paper into chad, typically either strips or fine particles in order to destroy private, confidential or otherwise sensitive Records. |
| **Security Management Plan** | the Supplier's security management plan prepared pursuant to Call-Off Schedule 9 (Security) (if applicable); |
| **Security Policy** | the Buyer's security policy, referred to in the Order Form, in force as at the Call-Off Start Date (a copy of which has been supplied to the Supplier), as updated from time to time and notified to the Supplier; |
| **Self Audit Certificate** | means the certificate in the form as set out in Framework Schedule 8 (Self Audit Certificate); |
| **Selection Criteria** | means information used to select whether a Record containing information of historical importance is suitable for Permanent |
| **Senior Sensitivity Reviewer** | means the Buyer's Head of Archive or alternative representative. |
| **Sensitive** | means kept secret or with restrictions on disclosure to avoid endangering security. |
| **Sensitivity Review** | means the process of conducting the review of Record(s) to identify sensitive information. |
| **Series Level Appraisal** | means the process of identifying Records containing historical information by reviewing the Buyers Records by series. |
| **Serious Fraud Office** | the UK Government body named as such as may be renamed or replaced by an equivalent body from time to time; |
| **"Service Levels"** | any service levels applicable to the provision of the Deliverables under the Call Off Contract (which, where Call Off Schedule 14 (Service Levels) is used in this Contract, are specified in the Annex to Part A of such Schedule); |
| **Service Lines** | means the list of Lines as defined in Lots 1, 2 4 and 5 of Framework Schedule 2. |
| **Service Period** | has the meaning given to it in the Order Form; |

| | |
|---|---|
| **Services** | services made available by the Supplier as specified in Framework Schedule 1 (Specification) and in relation to a Call-Off Contract as specified in the Order Form; |
| **Service Transfer** | any transfer of the Deliverables (or any part of the Deliverables), for whatever reason, from the Supplier or any Subcontractor to a Replacement Supplier or a Replacement Subcontractor; |
| **Service Transfer Date** | the date of a Service Transfer; |
| **Sift and Record Appraisal** | means an appraisal which will initially be conducted at Record Title, using Selection Criteria to identify Records containing information of historical importance |
| **Sites** | any premises (including the Buyer Premises, the Supplier's premises or third party premises) from, to or at which:<br>a) the Deliverables are (or are to be) provided; or<br>b) the Supplier manages, organises or otherwise directs the provision or the use of the Deliverables; |
| **Smarter Working** | means an approach to organising work that aims to drive greater efficiency and. effectiveness, enhancing personal and organisational outcomes through a combination of. flexibility, autonomy and collaboration, utilising a range of practices, technologies and working environments. |
| **SME** | an enterprise falling within the category of micro, small and medium sized enterprises defined by the Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium enterprises; |
| **Social Media** | means websites and applications that enable Users to create and share content or to participate in social networking. |
| **Software** | means the range of Software that has been specified within this Framework Agreement Schedule 2. |
| **Space Creation Activity** | means the Supplier identifying spaces within a Box(es) that incorporate more individual Record(s) and therefore reduce the number of Boxes the Buyer is being charged for storeage. |
| **Special Terms** | any additional Clauses set out in the Framework Award Form or Order Form which shall form part of the respective Contract; |

| | |
|---|---|
| **Specialist Records Management Service** | means the Services as defined with Lot 4 of Framework Schedule 2. |
| **Specific Change in Law** | a Change in Law that relates specifically to the business of the Buyer and which would not affect a Comparable Supply where the effect of that Specific Change in Law on the Deliverables is not reasonably foreseeable at the Start Date; |
| **Specification** | the specification set out in Framework Schedule 1 (Specification), as may, in relation to a Call-Off Contract, be supplemented by the Order Form; |
| **Standards** | any:<br>a) standards published by BSI British Standards, the National Standards Body of the United Kingdom, the International Organisation for Standardisation or other reputable or equivalent bodies (and their successor bodies) that a skilled and experienced operator in the same type of industry or business sector as the Supplier would reasonably and ordinarily be expected to comply with;<br>b) standards detailed in the specification in Schedule 1 (Specification);<br>c) standards detailed by the Buyer in the Order Form or agreed between the Parties from time to time;<br>d) relevant Government codes of practice and guidance applicable from time to time; |
| **Start Date** | in the case of the Framework Contract, the date specified on the Framework Award Form, and in the case of a Call-Off Contract, the date specified in the Order Form; |
| **Statement of Requirements** | a statement issued by the Buyer detailing its requirements in respect of Deliverables issued in accordance with the Call-Off Procedure; |
| **Storage Media** | the part of any device that is capable of storing and retrieving data; |

| | |
|---|---|
| **Sub-Contract** | any contract or agreement (or proposed contract or agreement), other than a Call-Off Contract or the Framework Contract, pursuant to which a third party:<br>a) provides the Deliverables (or any part of them);<br>b) provides facilities or services necessary for the provision of the Deliverables (or any part of them); and/or<br>c) is responsible for the management, direction or control of the provision of the Deliverables (or any part of them); |
| **Subcontractor** | any person other than the Supplier, who is a party to a Sub-Contract and the servants or agents of that person; |
| **Subprocessor** | any third Party appointed to process Personal Data on behalf of that Processor related to a Contract; |
| **Supplier** | the person, firm or company identified in the Framework Award Form; |
| **Supplier Action Plan** | means a document, maintained by the Authority, capturing information about the relationship between the Parties including, but not limited to strategic objectives, actions, initiatives, communication channels, risks and supplier performance. |
| **Supplier Assets** | all assets and rights used by the Supplier to provide the Deliverables in accordance with the Call-Off Contract but excluding the Buyer Assets; |
| **Supplier Authorised Representative** | the representative appointed by the Supplier named in the Framework Award Form, or later defined in a Call-Off Contract; |
| **Supplier's Confidential Information** | a) any information, however it is conveyed, that relates to the business, affairs, developments, IPR of the Supplier (including the Supplier Existing IPR) trade secrets, Know-How, and/or personnel of the Supplier;<br>b) any other information clearly designated as being confidential (whether or not it is marked as "confidential") or which ought reasonably to be considered to be confidential and which comes (or has come) to the Supplier's attention or into the Supplier's possession in connection with a Contract;<br>c) Information derived from any of (a) and (b) above; |
| **Supplier's Conract Manager "** | the person identified in the Order Form appointed by the Supplier to oversee the operation of the Call-Off Contract and any alternative person whom the Supplier intends to appoint to the role, provided that the Supplier informs the Buyer prior to the appointment; |

| | |
|---|---|
| **Supplier Equipment** | the Supplier's hardware, computer and telecoms devices, equipment, plant, materials and such other items supplied and used by the Supplier (but not hired, leased or loaned from the Buyer) in the performance of its obligations under this Call-Off Contract; |
| **Supplier Marketing Contact** | shall be the person identified in the Framework Award Form; |
| **Supplier Non-Performance** | where the Supplier has failed to:<br>a) Achieve a Milestone by its Milestone Date;<br>d) provide the Goods and/or Services in accordance with the Service Levels ; and/or<br>b) comply with an obligation under a Contract; |
| **Supplier Profit** | in relation to a period, the difference between the total Charges (in nominal cash flow terms but excluding any Deductions and total Costs (in nominal cash flow terms) in respect of a Call-Off Contract for the relevant period; |
| **Supplier Profit Margin** | in relation to a period or a Milestone (as the context requires), the Supplier Profit for the relevant period or in relation to the relevant Milestone divided by the total Charges over the same period or in relation to the relevant Milestone and expressed as a percentage; |
| **Supplier Relationship Management** | means the discipline of strategically and operationally planning for, and managing, all interactions with Suppliers that supply goods and services to the Authority via this Framework Agreement or Buyers via subsequent Call Off Contracts, in order to maximise the value of those interactions. |
| **Supplier Sensitivity Reports** | means a report to the Buyer's Senior Sensitivity Reviewer detailing findings of each Record reviewed and recommendations for considerations. |
| **Supplier Staff** | all directors, officers, employees, agents, consultants and contractors of the Supplier and/or of any Subcontractor engaged in the performance of the Supplier's obligations under a Contract; |
| **Supporting Documentation** | sufficient information in writing to enable the Buyer to reasonably assess whether the Charges, Reimbursable Expenses and other sums due from the Buyer under the Call-Off Contract detailed in the information are properly payable; |
| **Terms of Reference** | means the scope and limitations of a stated activity or area of knowledge |
| **Termination Notice** | a written notice of termination given by one Party to the other, notifying the Party receiving the notice of the intention of the Party |

| | |
|---|---|
| | giving the notice to terminate a Contract on a specified date and setting out the grounds for termination; |
| **Test Issue** | any variance or non-conformity of the Deliverables from their requirements as set out in a Call-Off Contract; |
| **Test Plan** | a plan:<br>a) for the Testing of the Deliverables; and<br>b) setting out other agreed criteria related to the achievement of Milestones; |
| **Tests** | any tests required to be carried out pursuant to a Call-Off Contract as set out in the Test Plan or elsewhere in a Call-Off Contract and "**Tested**" and "**Testing**" shall be construed accordingly; |
| **The National Archives** | means the non-ministerial government department who are the official archive and publisher for the UK government and guardians national documents |
| **Third Party Interim Resources** | means specialist resources provided by the Supplier through delivery of the Call Off contract. |
| **Third Party IPR** | Intellectual Property Rights owned by a third party which is or will be used by the Supplier for the purpose of providing the Deliverables; |
| **Title (procedure)** | means the process of identifying Records containing information by reviewing Buyer's Records by the Record name |
| **Transferring Supplier Employees** | those employees of the Supplier and/or the Supplier's Subcontractors to whom the Employment Regulations will apply on the Service Transfer Date; |
| **Transparency Information** | the Transparency Reports and the content of a Contract, including any changes to this Contract agreed from time to time, except for –<br>(i) any information which is exempt from disclosure in accordance with the provisions of the FOIA, which shall be determined by the Relevant Authority; an<br>(ii) Commercially Sensitive Information; |
| **Transparency Reports** | the information relating to the Deliverables and performance of the Contracts which the Supplier is required to provide to the Buyer in accordance with the reporting requirements in Call-Off Schedule 1 (Transparency Reports); |

| | |
|---|---|
| **Triage Sensitivity Service** | means the process of conducting the review of Record(s) to identify sensitive information and reporting recommendation(s) to the Buyers. |
| **Triage Sensitivity Reviewer** | means the process of determining the most important things from amongst a large number that require attention. Triage Sensitivity Reviewer |
| **Triage Sensitivity Project Manager** | means the Project Manager who oversees the Triage Sensitivity Reviewer and Triage Sensitivity Review process. |
| **UK Bank Holidays** | means all UK Bank Holidays which are detailed in the link below: https://www.gov.uk/bank-holidays |
| **User** | means either a member of Buyers' Personnel or Supplier employee |
| **Variation** | any change to a Contract; |
| **Variation Form** | the form set out in Joint Schedule 2 (Variation Form); |
| **Variation Procedure** | the procedure set out in Clause 24 (Changing the contract); |
| **VAT** | value added tax in accordance with the provisions of the Value Added Tax Act 1994; |
| **VCSE** | a non-governmental organisation that is value-driven and which principally reinvests its surpluses to further social, environmental or cultural objectives; |
| **Weeding Activity** | means checking content within the Buyer's Record(s) in order to identify specific information and/or content that can with removed from the Record(s). |
| **Whitehall** | is the name of a street in London in which there are many government offices. You can also use Whitehall to mean the British Government itself. |
| **Worker** | any one of the Supplier Staff which the Buyer, in its reasonable opinion, considers is an individual to which Procurement Policy Note 08/15 (Tax Arrangements of Public Appointees) (https://www.gov.uk/government/publications/procurement-policy-note-0815-tax-arrangements-of-appointees) applies in respect of the Deliverables; |
| **Working Day** | any day other than a Saturday or Sunday or public holiday in England and Wales unless specified otherwise by the Parties in the Order Form; |
| **Work Day** | 8.0 Work Hours, whether or not such hours are worked consecutively and whether or not they are worked on the same day; and |

| | |
|---|---|
| **Work Hours** | the hours spent by the Supplier Staff properly working on the provision of the Deliverables including time spent travelling (other than to and from the Supplier's offices, or to and from the Sites) but excluding lunch breaks. |

# Joint Schedule 2 (Variation Form)

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

| Contract Details | | |
|---|---|---|
| This variation is between: | **[delete** as applicable: CCS / Buyer**]** ("**CCS" "the Buyer"**)<br>And<br>**[insert** name of Supplier**]** (**"the Supplier"**) | |
| Contract name: | **[insert** name of contract to be changed**]** **("the Contract")** | |
| Contract reference number: | **[insert** contract reference number] | |
| **Details of Proposed Variation** | | |
| Variation initiated by: | **[delete** as applicable: CCS/Buyer/Supplier] | |
| Variation number: | **[insert** variation number] | |
| Date variation is raised: | **[insert** date] | |
| Proposed variation | | |
| Reason for the variation: | **[insert** reason] | |
| An Impact Assessment shall be provided within: | **[insert** number] days | |
| **Impact of Variation** | | |
| Likely impact of the proposed variation: | **[Supplier to insert** assessment of impact] | |
| **Outcome of Variation** | | |
| Contract variation: | This Contract detailed above is varied as follows:<br>● **[CCS/Buyer to insert** original Clauses or Paragraphs to be varied and the changed clause] | |
| Financial variation: | Original Contract Value: | £ **[insert** amount] |
| | Additional cost due to variation: | £ **[insert** amount] |
| | New Contract value: | £ **[insert** amount] |

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

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

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

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

Signature

Date

Name (in Capitals)

Address

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

Signature

Date

Name (in Capitals)

Address

# Joint Schedule 3 (Insurance Requirements)

## 1. The insurance you need to have

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

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

1.1.2 the Call-Off Contract Effective Date in respect of the Additional Insurances.

1.2 The Insurances shall be:

1.2.1 maintained in accordance with Good Industry Practice;

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

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

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

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

## 2. How to manage the insurance

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

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

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

2.1.3 hold all policies in respect of the Insurances and cause any insurance broker effecting the Insurances to hold any insurance slips and other evidence of placing cover representing any of the Insurances to which it is a party.

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

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

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

## 4. Evidence of insurance you must provide

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

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

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

## 6. Cancelled Insurance

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

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

## 7. Insurance claims

7.1 The Supplier shall promptly notify to insurers any matter arising from, or in relation to, the Deliverables, or each Contract for which it may be entitled to claim under any of the Insurances. In the event that the Relevant Authority receives a claim relating to or arising out of a Contract or the Deliverables, the Supplier shall co-operate with the Relevant Authority and assist it in dealing with such claims including without limitation providing information and documentation in a timely manner.

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

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

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

## ANNEX: REQUIRED INSURANCES

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

1.1 professional indemnity insurance [with cover (for a single event or a series of related events and in the aggregate) of not less than] five million pounds (£5,000,000). See below table as to which Lot this is required for;

1.2 public liability insurance [with cover (for a single event or a series of related events and in the aggregate)] of not less than five million pounds (£5,000,000). See below table as to which Lot this is required for;

1.3 employers' liability insurance [with cover (for a single event or a series of related events and in the aggregate) of not less than] five million pounds (£5,000,000). See below table as to which Lot this is required for; and

1.4 Product liability insurance [with cover (for a single event or a series of related events and in the aggregate) of not less than] five million pounds (£5,000,000). See below table as to which Lot this required for;

| | Lot 1 | Lot 2 | Lot 3 | Lot 4 | Lot 5 |
|---|---|---|---|---|---|
| Professional | ./ | ./ | ./ | ./ | ./ |
| Public | ./ | ./ | ./ | ./ | ./ |
| Employers liability | ./ | ./ | ./ | ./ | ./ |
| Product liability | ./ | ./ | ./ | | ./ |

# Joint Schedule 4 (Commercially Sensitive Information)

## 1. What is the Commercially Sensitive Information?

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

1.2 Where possible, the Parties have sought to identify when any relevant Information will cease to fall into the category of Information to which this Schedule applies in the table below and in the Order Form (which shall be deemed incorporated into the table below).

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

| No. | Date | Item(s) | Duration of Confidentiality |
|---|---|---|---|
| 1 | 1st June 2024 | Tender Response | Lifetime of contract |
| 2 | 1st June 2024 | Pricing Breakdown | Lifetime of contract |

| No. | Date | Item(s) | Duration of Confidentiality |
|---|---|---|---|
| | Call-Off Start Date | The pricing details set out in Call-Off Schedule 5 (Pricing Details) to this Call-Off Contract. | Until Contract Expiry |

| | | | |
|---|---|---|---|
| | Call-Off Start Date | The details of Supplier corporate structure, affiliates, sub-contractors and supply / procurement strategies. | Until Contract Expiry |
| | Call-Off Start Date | The details of Supplier innovative solutions or proposals; service delivery models; operating methodologies; working practices and Supplier site locations. | Until Contract Expiry |
| | Call-Off Start Date | Supplier intellectual property, including any proprietary software, data systems and online portals. | Until Contract Expiry |

# Joint Schedule 5 (Corporate Social Responsibility)

## 1. What we expect from our Suppliers

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

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

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

## 2. Equality and Accessibility

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

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

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

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

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

3.1 The Supplier:

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

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

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

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

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

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

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

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

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

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

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

## 4. Income Security

4.1 The Supplier shall:

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

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

4.1.3 All workers shall be provided with written and understandable Information about their employment conditions in respect of wages before they enter employment and about the particulars of their wages for the pay period concerned each time that they are paid;

4.1.4 not make deductions from wages:

(a) as a disciplinary measure

(b) except where permitted by law; or

(c) without expressed permission of the worker concerned;

4.1.5 record all disciplinary measures taken against Supplier Staff; and

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

## 5. Working Hours

5.1 The Supplier shall:

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

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

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

(a) the extent;

(b) frequency; and

(c) hours worked;

by individuals and by the Supplier Staff as a whole;

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

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

1.3.1 this is allowed by national law;

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

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

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

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

## 2. Sustainability

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

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

# Joint Schedule 6 (Key Subcontractors)

## 2. Restrictions on certain subcontractors

2.1 The Supplier is entitled to sub-contract its obligations under the Framework Contract to the Key Subcontractors set out in the Framework Award Form.

2.2 The Supplier is entitled to sub-contract its obligations under a Call-Off Contract to Key Subcontractors listed in the Framework Award Form who are specifically nominated in the Order Form.

2.3 Where during the Contract Period the Supplier wishes to enter into a new Key Sub-contract or replace a Key Subcontractor, it must obtain the prior written consent of CCS and the Buyer and the Supplier shall, at the time of requesting such consent, provide CCS and the Buyer with the information detailed in Paragraph 1.4. The decision of CCS and the Buyer to consent or not will not be unreasonably withheld or delayed. Where CCS consents to the appointment of a new Key Subcontractor then they will be added to section 18 of the Framework Award Form. Where the Buyer consents to the appointment of a new Key Subcontractor then they will be added to Key Subcontractor section of the Order Form. CCS and the Buyer may reasonably withhold their consent to the appointment of a Key Subcontractor if it considers that:

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

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

2.3.3 the proposed Key Subcontractor employs unfit persons.

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

2.4.1 the proposed Key Subcontractor's name, registered office and company registration number;

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

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

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

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

2.4.6 (where applicable) Credit Rating Threshold (as defined in Joint Schedule 7 (Financial Distress)) of the Key Subcontractor.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

# Joint Schedule 10 (Rectification Plan)

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

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

# Joint Schedule 11 (Processing Data)

## Status of the Controller

1. The Parties acknowledge that for the purposes of the Data Protection Legislation, the nature of the activity carried out by each of them in relation to their respective obligations under a Contract dictates the status of each party under the DPA 2018. A Party may act as:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(i) nature of the data to be protected;

(ii) harm that might result from a Personal Data Breach;

(iii) state of technological development; and

(iv) cost of implementing any measures;

(c) ensure that :

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

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

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

(B) are subject to appropriate confidentiality undertakings with the Processor or any Subprocessor;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(f) becomes aware of a Personal Data Breach.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(b) obtain the written consent of the Controller;

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

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

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

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

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

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

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

**Independent Controllers of Personal Data**

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

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

19. Where a Party has provided Personal Data to the other Party in accordance with paragraph 8 of this Joint Schedule 11 above, the recipient of the Personal Data will provide all such relevant documents and information relating to its data protection policies and procedures as the other Party may reasonably require.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

28. Notwithstanding the general application of paragraphs 2 to 15 of this Joint Schedule 11 to Personal Data, where the Supplier is required to exercise its regulatory and/or legal obligations in respect of Personal Data, it shall act as an Independent Controller of Personal Data in accordance with paragraphs 16 to 27 of this Joint Schedule 11.

## Annex 1 - Processing Personal Data

This Annex shall be completed by the Controller, who may take account of the view of the Processors, however the final decision as to the content of this Annex shall be with the Relevant Authority at its absolute discretion.

1.1 The contact details of the Relevant Authority's Data Protection Officer are: dataprotection@energysecurity.gov.uk

1.2 The contact details of the Supplier's Data Protection Officer are: [redacted]

1.3 The Processor shall comply with any further written instructions with respect to Processing by the Controller.

1.4 Any such further instructions shall be incorporated into this Annex.

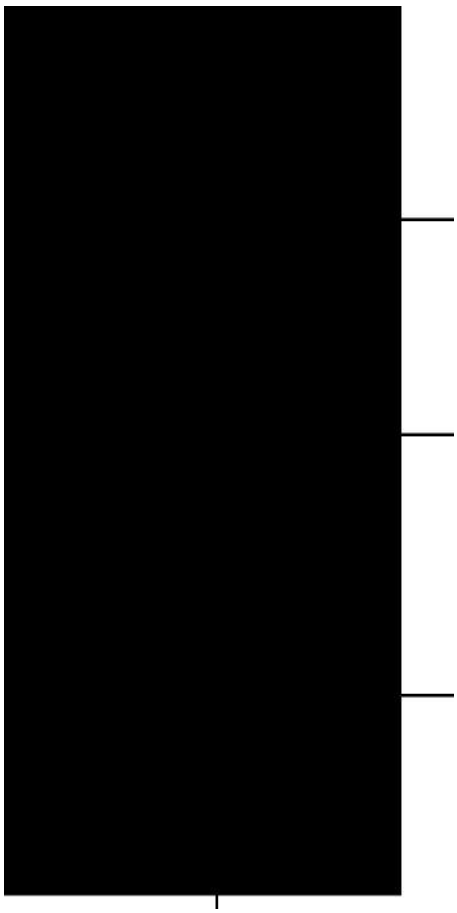
| Description | Details |
|---|---|
| Identity of Controller for each Category of Personal Data | **The Relevant Authority is Controller and the Supplier is Processor**<br><br>The Parties acknowledge that in accordance with paragraph 2 to paragraph 15 and for the purposes of the Data Protection Legislation, the Relevant Authority is the Controller and the Supplier is the Processor of the following Personal Data:<br><br>● Business contact details of Supplier Personnel for which the Supplier is the processor,<br><br>● Business contact details of any directors, officers, employees, agents. Consultants and contractors of CCS (excluding the Supplier Personnel) engaged in the performance of the CCS' duties under the Contract for which CCS is the Controller.<br><br>**The Parties are Independent Controllers of Personal Data** |

| | |
|---|---|
| | • *Business contact details of Supplier Personnel for which the Supplier is the Controller,*<br>• *Business contact details of any directors, officers, employees, agents, consultants and contractors of Relevant Authority (excluding the Supplier Personnel) engaged in the performance of the Relevant Authority's duties under the Contract) for which the Relevant Authority is the Controller,* |
| Duration of the Processing | The Framework Contract Period and thereafter, until expiry or termination of the last Call-Off Contract under the Framework, including the period until all transactions relating to Call-Off Contracts have permanently ceased. |
| Nature and purposes of the Processing | To facilitate the procurement of Goods and Services from the Framework Contract by public sector organisations and enable CCS to provide ongoing support and a point of escalation for Buyers in the day to day management of their individual Call-Off Contracts.<br><br>Day to day management and performance of obligations under the Framework Contract, including exit management and other associated activities. |
| Type of Personal Data | Personal details of each Party's Personnel engaged in the performance of obligations and day to day management of the<br><br>Framework Contract:<br><br>• Full name<br>• Job title<br>• Organisation name<br>• Business/workplace address<br>• Business/workplace email address<br>• Business/workplace telephone/mobile number(s)<br>• Supplier Personnel date of birth (when required for security<br>• purposes when Supplier Personnel visit CCS premises) |

| | |
|---|---|
| | • Supplier Dun & Bradstreet Data Universal Numbering System (DUNS number)<br>• Registered company details including registered company<br>• name, address and company registration number (CRN)<br>• Bank account details for activities related to the<br>• Management Charge<br>• Management Information |
| Categories of Data Subject | Personnel data of the Parties involved in the performance of obligations and day to day management of the Framework Contract. |
| Plan for return and destruction of the data once the Processing is complete<br><br>UNLESS requirement under Union or Member State law to preserve that type of data | Data will be retained for seven (7) years after the duration of the processing outlined above and in accordance with the CCS Privacy Notice.<br><br>In accordance with the Core Terms, all CCS data and any copies held by the Supplier must be securely erased once the Processing is complete, unless the Supplier is required by law to retain it.<br><br>In accordance with the Core Terms, all Storage Media that has held CCS data must be securely destroyed at the end of life of the media. All destruction of media must be in line with good industry practice. |
| Data Transfer | The Supplier agrees that they will not transfer Personal Data or Metadata outside of the EU unless the prior written consent of the Controller has been obtained |

The following are approved Subprocessors subject to clause 12 above:

| ENTITY (NAME & ADDRESS) | TYPE OF SERVICE PROVIDED | COUNTRY LOCATION[A1] |
|---|---|---|
| [redacted] | | |



# Joint Schedule 13 (Continuous Improvement)

## 1. Relevant Authority's Rights

1.1 The Relevant Authority and the Supplier recognise that, where specified in Framework Schedule 4 (Framework Management), the Relevant Authority may give CCS the right to enforce the Relevant Authority's rights under this Schedule.

## 2. Supplier's Obligations

2.1 The Supplier must, throughout the Contract Period, identify new or potential improvements to the provision of the Deliverables with a view to reducing the Relevant Authority's costs (including the Charges/Framework Prices) and/or improving the quality and efficiency of the Deliverables and their supply to the Relevant Authority.

2.2 The Supplier must adopt a policy of continuous improvement in relation to the Deliverables.

2.3 This may include regular reviews with the Relevant Authority of the Deliverables and the way it provides them, with a view to reducing the Relevant Authority's costs (including the Charges) and/or improving the quality and efficiency of the Deliverables. The Supplier and the Relevant Authority must provide each other with any information relevant to meeting this objective.

2.4 In addition to Paragraph 2.1, the Supplier may be requested by the Relevant Authority to produce at the start of each Contract (or where otherwise specified in the Order Form) a plan for improving the provision of Deliverables and/or reducing the Charges/Framework Prices (without adversely affecting the performance of this Contract) (**"Continuous Improvement Plan"**) for the Relevant Authority's approval. The Continuous Improvement Plan must include, as a minimum, proposals:

2.4.1 identifying the emergence of relevant new and evolving technologies;

2.4.2 changes in business processes of the Supplier or the Relevant Authority and ways of working that would provide cost savings and/or enhanced benefits to the Relevant Authority (such as methods of interaction, supply chain efficiencies, reduction in energy consumption and methods of sale);

2.4.3 new or potential improvements to the provision of the Deliverables including the quality, responsiveness, procedures, benchmarking methods, likely performance mechanisms and customer support services in relation to the Deliverables; and

2.4.4 measuring and reducing the sustainability impacts of the Supplier's operations and supply-chains relating to the

Deliverables, and identifying opportunities to assist the Relevant Authority in meeting their sustainability objectives.

2.4.5 improving the way in which the Goods and/or Services are sold via the Framework Agreement that may result in reduced Framework Prices;

2.4.6 identifying and implementing efficiencies in the Supplier's internal processes and administration that may lead to cost savings and reductions in the Framework Prices;

2.4.7 identifying and implementing efficiencies in the way CCS and/or the Relevant Authority interact with the Supplier that may lead to cost savings and reductions in the Framework Prices;

2.4.8 identifying and implementing efficiencies in the Supplier's supply chain that may lead to cost savings and reductions in the Framework Prices;

2.5 The initial Continuous Improvement Plan for the first (1st) Contract Year shall be submitted by the Supplier to the Relevant Authority for Approval within one hundred (100) Working Days of the first Order or six (6) Months following the Start Date, whichever is earlier.

2.6 The Relevant Authority reserves the right to request the initial Continuous Improvement Plan at any time during the Contract Period which may be after the first (1st) Contract Year, where it is deemed to be beneficial.

2.7 The Relevant Authority shall notify the Supplier of its approval or rejection of the proposed Continuous Improvement Plan or any updates to it within twenty (20) Working Days of receipt. If it is rejected then the Supplier shall, within ten (10) Working Days of receipt of notice of rejection, submit a revised Continuous Improvement Plan reflecting the changes required. Once Approved, it becomes the Continuous Improvement Plan for the purposes of this Contract.

2.8 The Supplier must provide sufficient information with each suggested improvement to enable a decision on whether to implement it. The Supplier shall provide any further information as requested.

2.9 If the Relevant Authority wishes to incorporate any improvement into this Contract, it must request a Variation in accordance with the Variation Procedure and the Supplier must implement such Variation at no additional cost to the Buyer or CCS.

2.10 Once the first Continuous Improvement Plan has been Approved in accordance with Paragraph 2.7:

2.10.1 the Supplier shall use all reasonable endeavours to implement any agreed deliverables in accordance with the Continuous Improvement Plan; and

2.10.2 the Parties agree to meet as soon as reasonably possible following the start of each quarter (or as otherwise agreed

between the Parties) to review the Supplier's progress against the Continuous Improvement Plan.

2.11 The Supplier shall update the Continuous Improvement Plan as and when required but at least once every Contract Year (after the first Continuous Improvement Plan has been approved) in accordance with the procedure and timescales set out in Paragraph 2.4.

2.12 All costs relating to the compilation or updating of the Continuous Improvement Plan and the costs arising from any improvement made pursuant to it and the costs of implementing any improvement, shall have no effect on and are included in the Charges.

2.13 Should the Supplier's costs in providing the Deliverables to the Relevant Authority be reduced as a result of any changes implemented, all of the cost savings shall be passed on to the Relevant Authority by way of a consequential and immediate reduction in the Charges for the Deliverables.

2.14 At any time during the Contract Period of the Call-Off Contract, the Supplier may make a proposal for gainshare and/or incentivisation. If the Relevant Authority deems gainshare and/or incentivisation to be applicable then the Supplier shall update the Continuous Improvement Plan so as to include details of the way in which the proposal shall be implemented in accordance with an agreed gainshare ratio.

# Joint Schedule 16 (Benchmarking)

## 3. DEFINITIONS

3.1 In this Schedule, the following expressions shall have the following meanings:

| | |
|---|---|
| **"Benchmark Review"** | a review of the Deliverables carried out in accordance with this Schedule to determine whether those Deliverables represent Good Value; |
| **"Benchmarked Deliverables"** | any Deliverables included within the scope of a Benchmark Review pursuant to this Schedule; |
| **"Comparable Rates"** | the Charges for Comparable Deliverables; |
| **"Comparable Deliverables"** | deliverables that are identical or materially similar to the Benchmarked Deliverables (including in terms of scope, specification, volume and quality of performance) provided that if no identical or materially similar Deliverables exist in the market, the Supplier shall propose an approach for developing a comparable Deliverables benchmark; |
| **"Comparison Group"** | a sample group of organisations providing Comparable Deliverables which consists of organisations which are either of similar size to the Supplier or which are similarly structured in terms of their business and their service offering so as to be fair comparators with the Supplier or which, are best practice organisations; |
| **"Equivalent Data"** | data derived from an analysis of the Comparable Rates and/or the Comparable Deliverables (as applicable) provided by the Comparison Group; |
| **"Good Value"** | that the Benchmarked Rates are within the Upper Quartile; and |
| **"Upper Quartile"** | in respect of Benchmarked Rates, that based on an analysis of Equivalent Data, the Benchmarked Rates, as compared to the range of prices for Comparable Deliverables, are within the top 25% in terms of best value for money for the recipients of Comparable Deliverables. |

## 4. When you should use this Schedule

4.1 The Supplier acknowledges that the Buyer wishes to ensure that the Deliverables, represent value for money to the taxpayer throughout the Contract Period.

4.2 This Schedule sets to ensure the Contracts represent value for money throughout and that the Buyer may terminate the Contract by issuing a Termination Notice to the Supplier if the Supplier refuses or fails to comply with its obligations as set out in Paragraphs 3 of this Schedule.

4.3 Amounts payable under this Schedule shall not fall with the definition of a Cost.

## 5. Benchmarking

### 5.1 How benchmarking works

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

5.1.2 The Buyer may, by written notice to the Supplier, require a Benchmark Review of any or all of the Deliverables.

5.1.3 The Buyer shall not be entitled to request a Benchmark Review during the first six (6) Month period from the Contract Commencement Date or at intervals of less than twelve (12) Months after any previous Benchmark Review.

5.1.4 The purpose of a Benchmark Review will be to establish whether the Benchmarked Deliverables are, individually and/or as a whole, Good Value.

5.1.5 The Deliverables that are to be the Benchmarked Deliverables will be identified by the Buyer in writing.

5.1.6 Upon its request for a Benchmark Review the Buyer shall nominate a benchmarker. The Supplier must approve the nomination within ten (10) Working Days unless the Supplier provides a reasonable explanation for rejecting the appointment. If the appointment is rejected then the Buyer may propose an alternative benchmarker. If the Parties cannot agree the appointment within twenty (20) days of the initial request for Benchmark review then a benchmarker shall be selected by the Chartered Institute of Financial Accountants.

5.1.7 The cost of a benchmarker shall be borne by the Buyer (provided that each Party shall bear its own internal costs of the Benchmark Review) except where the Benchmark Review demonstrates that the Benchmarked Service and/or the Benchmarked Deliverables are not Good Value, in which case the Parties shall share the cost of the benchmarker in such proportions as the Parties agree (acting reasonably). Invoices by the benchmarker shall be raised against the Supplier and the relevant portion shall be reimbursed by the Buyer.

## 5.2 Benchmarking Process

5.2.1 The benchmarker shall produce and send to the Buyer, for Approval, a draft plan for the Benchmark Review which must include:

(a) a proposed cost and timetable for the Benchmark Review;

(b) a description of the benchmarking methodology to be used which must demonstrate that the methodology to be used is capable of fulfilling the benchmarking purpose; and

(c) a description of how the benchmarker will scope and identify the Comparison Group.

5.2.2 The benchmarker, acting reasonably, shall be entitled to use any model to determine the achievement of value for money and to carry out the benchmarking.

5.2.3 The Buyer must give notice in writing to the Supplier within ten (10) Working Days after receiving the draft plan, advising the benchmarker and the Supplier whether it Approves the draft plan, or, if it does not approve the draft plan, suggesting amendments to that plan (which must be reasonable). If amendments are suggested then the benchmarker must produce an amended draft plan and this Paragraph 3.2.3 shall apply to any amended draft plan.

5.2.4 Once both Parties have approved the draft plan then they will notify the benchmarker. No Party may unreasonably withhold or delay its Approval of the draft plan.

5.2.5 Once it has received the Approval of the draft plan, the benchmarker shall:

(a) finalise the Comparison Group and collect data relating to Comparable Rates. The selection of the Comparable Rates (both in terms of number and identity) shall be a matter for the Supplier's professional judgment using:

(i) market intelligence;

(ii) the benchmarker's own data and experience;

(iii) relevant published information; and

(iv) pursuant to Paragraph 3.2.6 below, information from other suppliers or purchasers on Comparable Rates;

(b) by applying the adjustment factors listed in Paragraph 3.2.7 and from an analysis of the Comparable Rates, derive the Equivalent Data;

(c) using the Equivalent Data, calculate the Upper Quartile;

(d) determine whether or not each Benchmarked Rate is, and/or the Benchmarked Rates as a whole are, Good Value.

5.2.6 The Supplier shall use all reasonable endeavours and act in good faith to supply information required by the benchmarker in order to undertake the benchmarking. The Supplier agrees to use its

reasonable endeavours to obtain information from other suppliers or purchasers on Comparable Rates.

5.2.7 In carrying out the benchmarking analysis the benchmarker may have regard to the following matters when performing a comparative assessment of the Benchmarked Rates and the Comparable Rates in order to derive Equivalent Data:

(a) the contractual terms and business environment under which the Comparable Rates are being provided (including the scale and geographical spread of the customers);

(b) exchange rates;

(c) any other factors reasonably identified by the Supplier, which, if not taken into consideration, could unfairly cause the Supplier's pricing to appear non-competitive.

## 5.3 Benchmarking Report

5.3.1 For the purposes of this Schedule **"Benchmarking Report"** shall mean the report produced by the benchmarker following the Benchmark Review and as further described in this Schedule;

5.3.2 The benchmarker shall prepare a Benchmarking Report and deliver it to the Buyer, at the time specified in the plan Approved pursuant to Paragraph 3.2.3, setting out its findings. Those findings shall be required to:

(a) include a finding as to whether or not a Benchmarked Service and/or whether the Benchmarked Deliverables as a whole are, Good Value;

(b) if any of the Benchmarked Deliverables are, individually or as a whole, not Good Value, specify the changes that would be required to make that Benchmarked Service or the Benchmarked Deliverables as a whole Good Value; and

(c) include sufficient detail and transparency so that the Party requesting the Benchmarking can interpret and understand how the Supplier has calculated whether or not the Benchmarked Deliverables are, individually or as a whole, Good Value.

5.3.3 The Parties agree that any changes required to this Contract identified in the Benchmarking Report shall be implemented at the direction of the Buyer in accordance with Clause 24 (Changing the contract).

# Call-Off Schedule 1 (Transparency Reports)

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

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

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

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

# Annex A: List of Transparency Reports

| Title | Content | Format | Frequency |
|---|---|---|---|
| [redacted] | [redacted] | [redacted] | [redacted] |

# Call-Off Schedule 2 (Staff Transfer)

Buyers will need to ensure that appropriate provisions are included to deal with staff transfer on both entry and exit, and, irrespective of whether TUPE does apply on entry if there are employees eligible for New Fair Deal pension protection then the appropriate pensions provisions will also need to be selected.

If there is a staff transfer from the Buyer on entry (1st generation) then Part A shall apply.

If there is a staff transfer from former/incumbent supplier on entry (2nd generation), Part B shall apply.

If there is both a 1st and 2nd generation staff transfer on entry, then both Part A and Part B shall apply.

If either Part A and/or Part B apply, then consider whether Part D (Pensions) shall apply and the Buyer shall indicate on the Order Form which Annex shall apply (either D1 (CSPS), D2 (NHSPS), D3 (LGPS) or D4 (Other Schemes)). Part D pensions may also apply where there is not a TUPE transfer for example where the incumbent provider is successful.

If there is no staff transfer (either 1st generation or 2nd generation) at the Start Date then Part C shall apply and Part D pensions may also apply where there is not a TUPE transfer for example where the incumbent provider is successful.

If the position on staff transfers is not known at the bid stage, include Parts A, B, C and D at the bid stage and then update the Buyer Contract Details before signing to specify whether Parts A and/or B, or C and D apply to the Contract.

Part E (dealing with staff transfer on exit) shall apply to every Contract.

For further guidance on this Schedule contact Government Legal Department's Employment Law Group]

## 1. Definitions

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

| | |
|---|---|
| **"Acquired Rights Directive"** | the European Council Directive 77/187/EEC on the approximation of laws of European member states relating to the safeguarding of employees' rights in the event of transfers of undertakings, businesses or parts of undertakings or businesses, as amended or re-enacted from time to time; |
| **"Employee Liability"** | all claims, actions, proceedings, orders, demands, complaints, investigations (save for any claims for personal injury which are covered by insurance) and any award, compensation, damages, tribunal awards, fine, loss, order, penalty, disbursement, payment made by way of settlement and costs, expenses and legal costs reasonably incurred in connection with a claim or investigation including in relation to the following:<br>redundancy payments including contractual or enhanced redundancy costs, termination costs and notice payments;<br>unfair, wrongful or constructive dismissal compensation;<br>compensation for discrimination on grounds of sex, race, disability, age, religion or belief, gender reassignment, marriage or civil partnership, pregnancy and maternity or sexual orientation or claims for equal pay;<br>compensation for less favourable treatment of part-time workers or fixed term employees;<br>outstanding employment debts and unlawful deduction of wages including any PAYE and National Insurance Contributions; |

employment claims whether in tort, contract or statute or otherwise;

any investigation relating to employment matters by the Equality and Human Rights Commission or other enforcement, regulatory or supervisory body and of implementing any requirements which may arise from such investigation;

**"Former Supplier"** a supplier supplying services to the Buyer before the Relevant Transfer Date that are the same as or substantially similar to the Services (or any part of the Services) and shall include any Subcontractor of such supplier (or any Subcontractor of any such Subcontractor);

**"New Fair Deal"** the revised Fair Deal position set out in the HM Treasury guidance: "*Fair Deal for Staff Pensions: Staff Transfer from Central Government*" issued in October 2013 including:

any amendments to that document immediately prior to the Relevant Transfer Date; and

any similar pension protection in accordance with the Annexes D1-D3 inclusive to Part D of this Schedule as notified to the Supplier by the Buyer;

**"Old Fair Deal"** HM Treasury Guidance "*Staff Transfers from Central Government: A Fair Deal for Staff Pensions*" issued in June 1999 including the supplementary guidance "*Fair Deal for Staff pensions: Procurement of Bulk Transfer Agreements and Related Issues*" issued in June 2004;

**"Partial Termination"** the partial termination of the relevant Contract to the extent that it relates to the provision of any part of the Services as further provided for in Clause 10.4 (When CCS or the Buyer can end this contract) or 10.6 (When the Supplier can end the contract);

**"Relevant Transfer"** a transfer of employment to which the Employment Regulations applies;

| | |
|---|---|
| **"Relevant Transfer Date"** | n relation to a Relevant Transfer, the date upon which the Relevant Transfer takes place. For the purposes of Part D: Pensions and its Annexes, where the Supplier or a Subcontractor was the Former Supplier and there is no Relevant Transfer of the Fair Deal Employees because they remain continuously employed by the Supplier (or Subcontractor), references to the Relevant Transfer Date shall become references to the Start Date; |
| **"Staffing Information"** | in relation to all persons identified on the Supplier's Provisional Supplier Personnel List or Supplier's Final Supplier Personnel List, as the case may be, such information as the Buyer may reasonably request (subject to all applicable provisions of the Data Protection Legislation), but including in an anonymised format:<br>(a) their ages, dates of commencement of employment or engagement, gender and place of work;<br>(b) details of whether they are employed, self-employed contractors or consultants, agency workers or otherwise;<br>(c) the identity of the employer or relevant contracting Party;<br>(d) their relevant contractual notice periods and any other terms relating to termination of employment, including redundancy procedures, and redundancy payments;<br>(e) their wages, salaries, bonuses and profit sharing arrangements as applicable;<br>(f) details of other employment-related benefits, including (without limitation) medical insurance, life assurance, pension or other retirement benefit schemes, share option schemes and company car schedules applicable to them;<br>(g) any outstanding or potential contractual, statutory or other liabilities in respect of such individuals (including in respect of personal injury claims); |

(h) details of any such individuals on long term sickness absence, parental leave, maternity leave or other authorised long term absence;

(i) copies of all relevant documents and materials relating to such information, including copies of relevant contracts of employment (or relevant standard contracts if applied generally in respect of such employees); and

(j) any other "employee liability information" as such term is defined in regulation 11 of the Employment Regulations;

| | |
|---|---|
| **"Supplier's Final Supplier Personnel List"** | a list provided by the Supplier of all Supplier Staff whose will transfer under the Employment Regulations on the Service Transfer Date; |
| **"Supplier's Provisional Supplier Personnel List"** | a list prepared and updated by the Supplier of all Supplier Staff who are at the date of the list wholly or mainly engaged in or assigned to the provision of the Services or any relevant part of the Services which it is envisaged as at the date of such list will no longer be provided by the Supplier; |
| **"Term"** | the period commencing on the Start Date and ending on the expiry of the Initial Period or any Extension Period or on earlier termination of the relevant Contract; |
| **"Transferring Buyer Employees"** | those employees of the Buyer to whom the Employment Regulations will apply on the Relevant Transfer Date; |
| **"Transferring Former Supplier Employees"** | in relation to a Former Supplier, those employees of the Former Supplier to whom the Employment Regulations will apply on the Relevant Transfer Date. |

## 2. INTERPRETATION

2.1 Where a provision in this Schedule imposes any obligation on the Supplier including (without limit) to comply with a requirement or provide an indemnity, undertaking or warranty, the Supplier shall procure that each of its Subcontractors shall comply with such obligation and provide such indemnity, undertaking or warranty to CCS, the Buyer, Former Supplier, Replacement Supplier or Replacement Subcontractor, as the case may be and where the Subcontractor fails to satisfy any claims under such

indemnities the Supplier will be liable for satisfying any such claim as if it had provided the indemnity itself.

2.2 The provisions of Paragraphs 2.1 and 2.6 of Part A, Paragraph 3.1 of Part B, Paragraphs 1.5, 1.7 and 1.9 of Part C, Part D and Paragraphs 1.4, 2.3 and 2.8 of Part E of this Schedule (together "Third Party Provisions") confer benefits on third parties (each such person a "Third Party Beneficiary") and are intended to be enforceable by Third Party Beneficiaries by virtue of the CRTPA.

2.3 Subject to Paragraph 2.2 above, a person who is not a Party to this Call-Off Contract has no right under the CRTPA to enforce any term of this Call-Off Contract but this does not affect any right or remedy of any person which exists or is available otherwise than pursuant to that Act.

2.4 No Third Party Beneficiary may enforce, or take any step to enforce, any Third Party Provision without the prior written consent of the Buyer, which may, if given, be given on and subject to such terms as the Buyer may determine.

2.5 Any amendments or modifications to this Call-Off Contract may be made, and any rights created under Paragraph 2.2 above may be altered or extinguished, by the Parties without the consent of any Third Party Beneficiary.

**3. Which parts of this Schedule apply**

Only the following parts of this Schedule shall apply to this Call Off Contract:

- *Part C (No Staff Transfer on the Start Date)*
- *Part E (Staff Transfer on Exit)*

# Part A: Staff Transfer at the Start Date

# Outsourcing from the Buyer

### 1. What is a relevant transfer

1.1 The Buyer and the Supplier agree that:

1.1.1 the commencement of the provision of the Services or of each relevant part of the Services will be a Relevant Transfer in relation to the Transferring Buyer Employees; and

1.1.2 as a result of the operation of the Employment Regulations, the contracts of employment between the Buyer and the Transferring Buyer Employees (except in relation to any terms disapplied through operation of regulation 10(2) of the Employment Regulations) will have effect on and from the Relevant Transfer Date as if originally made between the Supplier and/or any Sub-contractor and each such Transferring Buyer Employee.

1.2 The Buyer shall comply with all its obligations under the Employment Regulations and shall perform and discharge all its obligations in respect of the Transferring Buyer Employees in respect of the period arising up to (but not including) the Relevant Transfer Date (including (without limit) the payment of all remuneration, benefits, entitlements and outgoings, all wages, accrued but untaken holiday pay, bonuses, commissions, payments of PAYE, national insurance contributions and pension contributions which in any case are attributable in whole or in part to the period up to (but not including) the Relevant Transfer Date) and any necessary apportionments in respect of any periodic payments shall be made between: (i) the Buyer; and (ii) the Supplier and/or any Subcontractor (as appropriate).

### 29. Indemnities the Buyer must give

2.1 Subject to Paragraph 2.2, the Buyer shall indemnify the Supplier and any Subcontractor against any Employee Liabilities arising from or as a result of:

2.1.1 any act or omission by the Buyer in respect of any Transferring Buyer Employee or any appropriate employee representative (as defined in the Employment Regulations) of any Transferring Buyer Employee occurring before the Relevant Transfer Date;

2.1.2 the breach or non-observance by the Buyer before the Relevant Transfer Date of:

(a) any collective agreement applicable to the Transferring Buyer Employees; and/or

(b) any custom or practice in respect of any Transferring Buyer Employees which the Buyer is contractually bound to honour;

2.1.3 any claim by any trade union or other body or person representing the Transferring Buyer Employees arising from or connected with any failure by the Buyer to comply with any legal obligation to such trade union, body or person arising before the Relevant Transfer Date;

2.1.4 any proceeding, claim or demand by HMRC or other statutory authority in respect of any financial obligation including, but not limited to, PAYE and primary and secondary national insurance contributions:

(a) in relation to any Transferring Buyer Employee, to the extent that the proceeding, claim or demand by HMRC or other statutory authority relates to financial obligations arising before the Relevant Transfer Date; and

(b) in relation to any employee who is not a Transferring Buyer Employee and in respect of whom it is later alleged or determined that the Employment Regulations applied so as to transfer his/her employment from the Buyer to the Supplier and/or any Subcontractor as appropriate, to the extent that the proceeding, claim or demand by the HMRC or other statutory authority relates to financial obligations arising before the Relevant Transfer Date.

2.1.5 a failure of the Buyer to discharge, or procure the discharge of, all wages, salaries and all other benefits and all PAYE tax deductions and national insurance contributions relating to the Transferring Buyer Employees arising before the Relevant Transfer Date;

2.1.6 any claim made by or in respect of any person employed or formerly employed by the Buyer other than a Transferring Buyer Employee for whom it is alleged the Supplier and/or any Subcontractor as appropriate may be liable by virtue of the Employment Regulations and/or the Acquired Rights Directive; and

2.1.7 any claim made by or in respect of a Transferring Buyer Employee or any appropriate employee representative (as defined in the Employment Regulations) of any Transferring Buyer Employee relating to any act or omission of the Buyer in relation to its obligations under regulation 13 of the Employment Regulations, except to the extent that the liability arises from the failure by the Supplier or any Subcontractor to comply with regulation 13(4) of the Employment Regulations.

2.2 The indemnities in Paragraph 2.1 shall not apply to the extent that the Employee Liabilities arise or are attributable to an act or omission of the Supplier or any Subcontractor whether occurring or having its origin before, on or after the Relevant Transfer Date including any Employee Liabilities:

2.2.1 arising out of the resignation of any Transferring Buyer Employee before the Relevant Transfer Date on account of substantial detrimental changes to his/her working conditions proposed by the Supplier and/or any Subcontractor to occur in the period from (and including) the Relevant Transfer Date; or

2.2.2 arising from the failure by the Supplier or any Subcontractor to comply with its obligations under the Employment Regulations.

2.3 If any person who is not identified by the Buyer as a Transferring Buyer Employee claims, or it is determined in relation to any person who is not identified by the Buyer as a Transferring Buyer Employee, that his/her contract of employment has been transferred from the Buyer to the Supplier and/or any Subcontractor pursuant to the Employment Regulations or the Acquired Rights Directive then:

2.3.1 the Supplier shall, or shall procure that the Subcontractor shall, within 5 Working Days of becoming aware of that fact, notify the Buyer in writing; and

2.3.2 the Buyer may offer (or may procure that a third party may offer) employment to such person, or take such other reasonable steps as the Buyer considers appropriate to deal with the matter provided always that such steps are in compliance with Law, within 15 Working Days of receipt of notice from the Supplier and/or any Subcontractor.

2.4 If an offer referred to in Paragraph 2.3.2 is accepted, or if the situation has otherwise been resolved by the Buyer, the Supplier shall, or shall procure that a Subcontractor shall, immediately release the person from his/her employment or alleged employment;

2.5 If by the end of the 15 Working Day period referred to in Paragraph 2.3.2:

2.5.1 no such offer of employment has been made;

2.5.2 such offer has been made but not accepted; or

2.5.3 the situation has not otherwise been resolved,

the Supplier and/or any Subcontractor may within 5 Working Days give notice to terminate the employment or alleged employment of such person.

2.6 Subject to the Supplier and/or any Subcontractor acting in accordance with the provisions of Paragraphs 2.3 to 2.5 and in accordance with all applicable proper employment procedures set out in applicable Law and

subject also to Paragraph 2.7, the Buyer will indemnify the Supplier and/or the relevant Subcontractor against all Employee Liabilities arising out of the termination of the employment pursuant to the provisions of Paragraph 2.5 provided that the Supplier takes, or procures that the Subcontractor takes, all reasonable steps to minimise any such Employee Liabilities.

2.7 The indemnity in Paragraph 2.6:

2.7.1 shall not apply to:

(a) any claim for:

(i) discrimination, including on the grounds of sex, race, disability, age, gender reassignment, marriage or civil partnership, pregnancy and maternity or sexual orientation, religion or belief; or

(ii) equal pay or compensation for less favourable treatment of part-time workers or fixed-term employees;

in any case in relation to any alleged act or omission of the Supplier and/or any Subcontractor; or

(b) any claim that the termination of employment was unfair because the Supplier and/or any Subcontractor neglected to follow a fair dismissal procedure; and

2.7.2 shall apply only where the notification referred to in Paragraph 2.3.1 is made by the Supplier and/or any Subcontractor (as appropriate) to the Buyer within 6 months of the Start Date

2.8 If any such person as is referred to in Paragraph 2.3 is neither re-employed by the Buyer nor dismissed by the Supplier and/or any Subcontractor within the time scales set out in Paragraph 2.5, such person shall be treated as having transferred to the Supplier and/or any Subcontractor and the Supplier shall, or shall procure that the relevant Subcontractor shall, comply with such obligations as may be imposed upon it under applicable Law.

**3. Indemnities the Supplier must give and its obligations**

3.1 Subject to Paragraph 3.2, the Supplier shall indemnify the Buyer against any Employee Liabilities arising from or as a result of:

3.1.1 any act or omission by the Supplier or any Subcontractor in respect of any Transferring Buyer Employee or any appropriate employee representative (as defined in the Employment Regulations) of any Transferring Buyer Employee whether occurring before, on or after the Relevant Transfer Date;

3.1.2 the breach or non-observance by the Supplier or any Subcontractor on or after the Relevant Transfer Date of:

(a) any collective agreement applicable to the Transferring Buyer Employees; and/or

(b) any custom or practice in respect of any Transferring Buyer Employees which the Supplier or any Subcontractor is contractually bound to honour;

3.1.3 any claim by any trade union or other body or person representing any Transferring Buyer Employees arising from or connected with any failure by the Supplier or any Subcontractor to comply with any legal obligation to such trade union, body or person arising on or after the Relevant Transfer Date;

3.1.4 any proposal by the Supplier or a Subcontractor made before the Relevant Transfer Date to make changes to the terms and conditions of employment or working conditions of any Transferring Buyer Employees to their material detriment on or after their transfer to the Supplier or the relevant Subcontractor (as the case may be) on the Relevant Transfer Date, or to change the terms and conditions of employment or working conditions of any person who would have been a Transferring Buyer Employee but for their resignation (or decision to treat their employment as terminated under regulation 4(9) of the Employment Regulations) before the Relevant Transfer Date as a result of or for a reason connected to such proposed changes;

3.1.5 any statement communicated to or action undertaken by the Supplier or any Subcontractor to, or in respect of, any Transferring Buyer Employee before the Relevant Transfer Date regarding the Relevant Transfer which has not been agreed in advance with the Buyer in writing;

3.1.6 any proceeding, claim or demand by HMRC or other statutory authority in respect of any financial obligation including, but not limited to, PAYE and primary and secondary national insurance contributions:

(a) in relation to any Transferring Buyer Employee, to the extent that the proceeding, claim or demand by HMRC or other statutory authority relates to financial obligations arising on or after the Relevant Transfer Date; and

(b) in relation to any employee who is not a Transferring Buyer Employee, and in respect of whom it is later alleged or determined that the Employment Regulations applied so as to transfer his/her employment from the Buyer to the Supplier or a

Subcontractor, to the extent that the proceeding, claim or demand by HMRC or other statutory authority relates to financial obligations arising on or after the Relevant Transfer Date;

3.1.7 a failure of the Supplier or any Subcontractor to discharge or procure the discharge of all wages, salaries and all other benefits and all PAYE tax deductions and national insurance contributions relating to the Transferring Author Buyer ity Employees in respect of the period from (and including) the Relevant Transfer Date;

3.1.8 any claim made by or in respect of a Transferring Buyer Employee or any appropriate employee representative (as defined in the Employment Regulations) of any Transferring Buyer Employee relating to any act or omission of the Supplier or any Subcontractor in relation to their obligations under regulation 13 of the Employment Regulations, except to the extent that the liability arises from the Buyer's failure to comply with its obligations under regulation 13 of the Employment Regulations; and

3.1.9 a failure by the Supplier or any Sub-contractor to comply with its obligations under paragraph 2.8 above.

3.2 The indemnities in Paragraph 3.1 shall not apply to the extent that the Employee Liabilities arise or are attributable to an act or omission of the Buyer whether occurring or having its origin before, on or after the Relevant Transfer Date including, without limitation, any Employee Liabilities arising from the Buyer's failure to comply with its obligations under the Employment Regulations.

3.3 The Supplier shall comply, and shall procure that each Subcontractor shall comply, with all its obligations under the Employment Regulations (including its obligation to inform and consult in accordance with regulation 13 of the Employment Regulations) and shall perform and discharge, and shall procure that each Subcontractor shall perform and discharge, all its obligations in respect of the Transferring Buyer Employees, from (and including) the Relevant Transfer Date (including (without limit) the payment of all remuneration, benefits, entitlements and outgoings, all wages, accrued but untaken holiday pay, bonuses, commissions, payments of PAYE, national insurance contributions and pension contributions which in any case are attributable in whole or in part to the period from and including the Relevant Transfer Date) and any necessary apportionments in respect of any periodic payments shall be made between the Buyer and the Supplier.

## 4. Information the Supplier must provide

4.1 The Supplier shall, and shall procure that each Subcontractor shall, promptly provide to the Buyer in writing such information as is necessary to enable the Buyer to carry out its duties under regulation 13 of the Employment Regulations. The Buyer shall promptly provide to the Supplier

and any Subcontractor in writing such information as is necessary to enable the Supplier and any Subcontractor to carry out their respective duties under regulation 13 of the Employment Regulations.

## 5. Cabinet Office requirements

5.1 The Parties agree that the Principles of Good Employment Practice issued by the Cabinet Office in December 2010 apply to the treatment by the Supplier of employees whose employment begins after the Relevant Transfer Date, and the Supplier undertakes to treat such employees in accordance with the provisions of the Principles of Good Employment Practice.

5.2 The Supplier shall, and shall procure that each Subcontractor shall, comply with any requirement notified to it by the Buyer relating to pensions in respect of any Transferring Buyer Employee as set down in:

5.2.1 the Cabinet Office Statement of Practice on Staff Transfers in the Public Sector of January 2000, revised December 2013;

5.2.2 Old Fair Deal; and/or

5.2.3 The New Fair Deal.

5.3 Any changes embodied in any statement of practice, paper or other guidance that replaces any of the documentation referred to in Paragraphs 5.1 or 5.2 shall be agreed in accordance with the Variation Procedure.

## 6. Pensions

6.1 The Supplier shall, and/or shall procure that each of its Subcontractors shall, comply with:

6.1.1 the requirements of Part 1 of the Pensions Act 2008, section 258 of the Pensions Act 2004 and the Transfer of Employment (Pension Protection) Regulations 2005 for all transferring staff; and

6.1.2 Part D: Pensions (and its Annexes) to this Schedule.

# Part C: No Staff Transfer on the Start Date

### 1. What happens if there is a staff transfer

1.1 The Buyer and the Supplier agree that the commencement of the provision of the Services or of any part of the Services will not be a Relevant Transfer in relation to any employees of the Buyer and/or any Former Supplier.

1.2 If any employee of the Buyer and/or a Former Supplier claims, or it is determined in relation to any employee of the Buyer and/or a Former Supplier, that his/her contract of employment has been transferred from the Buyer and/or the Former Supplier to the Supplier and/or any Subcontractor pursuant to the Employment Regulations or the Acquired Rights Directive then:

1.2.1 the Supplier shall, and shall procure that the relevant Subcontractor shall, within 5 Working Days of becoming aware of that fact, notify the Buyer in writing and, where required by the Buyer, notify the Former Supplier in writing; and

1.2.2 the Buyer and/or the Former Supplier may offer (or may procure that a third party may offer) employment to such person within 15 Working Days of the notification from the Supplier or the Subcontractor (as appropriate) or take such other reasonable steps as the Buyer or Former Supplier (as the case may be) it considers appropriate to deal with the matter provided always that such steps are in compliance with applicable Law.

1.3 If an offer referred to in Paragraph 1.2.2 is accepted (or if the situation has otherwise been resolved by the Buyer and/or the Former Supplier),, the Supplier shall, or shall procure that the Subcontractor shall, immediately release the person from his/her employment or alleged employment.

1.4 If by the end of the 15 Working Day period referred to in Paragraph 1.2.2:

1.4.1 no such offer of employment has been made;

1.4.2 such offer has been made but not accepted; or

1.4.3 the situation has not otherwise been resolved;

the Supplier may within 5 Working Days give notice to terminate the employment or alleged employment of such person.

1.5 Subject to the Supplier and/or the relevant Subcontractor acting in accordance with the provisions of Paragraphs 1.2 to 1.4 and in accordance with all applicable employment procedures set out in applicable Law and subject also to Paragraph 1.8 the Buyer shall:

1.5.1 indemnify the Supplier and/or the relevant Subcontractor against all Employee Liabilities arising out of the termination of the employment of any of the Buyer's employees referred

to in Paragraph 1.2 made pursuant to the provisions of Paragraph 1.4 provided that the Supplier takes, or shall procure that the Subcontractor takes, all reasonable steps to minimise any such Employee Liabilities; and

1.5.2 procure that the Former Supplier indemnifies the Supplier and/or any Subcontractor against all Employee Liabilities arising out of termination of the employment of the employees of the Former Supplier referred to in Paragraph 1.2 made pursuant to the provisions of Paragraph 1.4 provided that the Supplier takes, or shall procure that the relevant Subcontractor takes, all reasonable steps to minimise any such Employee Liabilities.

1.6 If any such person as is described in Paragraph 1.2 is neither re employed by the Buyer and/or the Former Supplier as appropriate nor dismissed by the Supplier and/or any Subcontractor within the 15 Working Day period referred to in Paragraph 1.4 such person shall be treated as having transferred to the Supplier and/or the Subcontractor (as appropriate) and the Supplier shall, or shall procure that the Subcontractor shall, comply with such obligations as may be imposed upon it under Law.

1.7 Where any person remains employed by the Supplier and/or any Subcontractor pursuant to Paragraph 1.6, all Employee Liabilities in relation to such employee shall remain with the Supplier and/or the Subcontractor and the Supplier shall indemnify the Buyer and any Former Supplier, and shall procure that the Subcontractor shall indemnify the Buyer and any Former Supplier, against any Employee Liabilities that either of them may incur in respect of any such employees of the Supplier and/or employees of the Subcontractor.

1.8 The indemnities in Paragraph 1.5:

1.8.1 shall not apply to:

(a) any claim for:

(i) discrimination, including on the grounds of sex, race, disability, age, gender reassignment, marriage or civil partnership, pregnancy and maternity or sexual orientation, religion or belief; or

( ) equal pay or compensation for less favourable treatment of part-time workers or fixed-term employees,

in any case in relation to any alleged act or omission of the Supplier and/or Subcontractor; or

(b) any claim that the termination of employment was unfair because the Supplier and/or any Subcontractor neglected to follow a fair dismissal procedure; and

1.8.2 shall apply only where the notification referred to in Paragraph 1.2.1 is made by the Supplier and/or any Subcontractor to the Buyer and, if applicable, Former Supplier within 6 months of the Start Date.

1.9 If the Supplier and/or the Subcontractor does not comply with Paragraph 1.2, all Employee Liabilities in relation to such employees shall remain with the Supplier and/or the Subcontractor and the Supplier shall (i) comply with the provisions of Part D: Pensions of this Schedule, and (ii) indemnify the Buyer and any Former Supplier against any Employee Liabilities that either of them may incur in respect of any such employees of the Supplier and/or employees of the Subcontractor.

## 2. Limits on the Former Supplier's obligations

Where in this Part C the Buyer accepts an obligation to procure that a Former Supplier does or does not do something, such obligation shall be limited so that it extends only to the extent that the Buyer's contract with the Former Supplier contains a contractual right in that regard which the Buyer may enforce, or otherwise so that it requires only that the Buyer must use reasonable endeavours to procure that the Former Supplier does or does not act accordingly.

# Part E: Staff Transfer on Exit

## 1. Obligations before a Staff Transfer

1.1 The Supplier agrees that within 20 Working Days of the earliest of:

1.1.1 receipt of a notification from the Buyer of a Service Transfer or intended Service Transfer;

1.1.2 receipt of the giving of notice of early termination or any Partial Termination of the relevant Contract;

1.1.3 the date which is 12 Months before the end of the Term; and

1.1.4 receipt of a written request of the Buyer at any time (provided that the Buyer shall only be entitled to make one such request in any 6 Month period),

it shall provide in a suitably anonymised format so as to comply with the Data Protection Legislation, the Supplier's Provisional Supplier Personnel List, together with the Staffing Information in relation to the Supplier's Provisional Supplier Personnel List and it shall provide an updated Supplier's Provisional Supplier Personnel List at such intervals as are reasonably requested by the Buyer.

1.2 At least 20 Working Days prior to the Service Transfer Date, the Supplier shall provide to the Buyer or at the direction of the Buyer to any Replacement Supplier and/or any Replacement Subcontractor (i) the Supplier's Final Supplier Personnel List, which shall identify the basis upon which they are Transferring Supplier Employees and (ii) the Staffing Information in relation to the Supplier's Final Supplier Personnel List (insofar as such information has not previously been provided).

1.3 The Buyer shall be permitted to use and disclose information provided by the Supplier under Paragraphs 1.1 and 1.2 for the purpose of informing any prospective Replacement Supplier and/or Replacement Subcontractor.

1.4 The Supplier warrants, for the benefit of The Buyer, any Replacement Supplier, and any Replacement Subcontractor that all information provided pursuant to Paragraphs 1.1 and 1.2 shall be true and accurate in all material respects at the time of providing the information.

1.5 From the date of the earliest event referred to in Paragraph 1.1.1, 1.1.2 and 1.1.3, the Supplier agrees that it shall not, and agrees to procure that each Subcontractor shall not, assign any person to the provision of the Services who is not listed on the Supplier's Provisional Supplier Personnel List and shall not without the approval of the Buyer (not to be unreasonably withheld or delayed):

:

1.5.1 replace or re-deploy any Supplier Staff listed on the Supplier Provisional Supplier Personnel List other than where any replacement is of equivalent grade, skills, experience and

expertise and is employed on the same terms and conditions of employment as the person he/she replaces

1.5.2 make, promise, propose, permit or implement any material changes to the terms and conditions of employment of the Supplier Staff (including pensions and any payments connected with the termination of employment);

1.5.3 increase the proportion of working time spent on the Services (or the relevant part of the Services) by any of the Supplier Staff save for fulfilling assignments and projects previously scheduled and agreed;

1.5.4 introduce any new contractual or customary practice concerning the making of any lump sum payment on the termination of employment of any employees listed on the Supplier's Provisional Supplier Personnel List;

1.5.5 increase or reduce the total number of employees so engaged, or deploy any other person to perform the Services (or the relevant part of the Services);

1.5.6 terminate or give notice to terminate the employment or contracts of any persons on the Supplier's Provisional Supplier Personnel List save by due disciplinary process;

and shall promptly notify, and procure that each Subcontractor shall promptly notify, the Buyer or, at the direction of the Buyer, any Replacement Supplier and any Replacement Subcontractor of any notice to terminate employment given by the Supplier or relevant Subcontractor or received from any persons listed on the Supplier's Provisional Supplier Personnel List regardless of when such notice takes effect.

1.6 On or around each anniversary of the Start Date and up to four times during the last 12 Months of the Term, the Buyer may make written requests to the Supplier for information relating to the manner in which the Services are organised. Within 20 Working Days of receipt of a written request the Supplier shall provide, and shall procure that each Subcontractor shall provide, to the Buyersuch information as the Buyer may reasonably require relating to the manner in which the Services are organised, which shall include:

1.6.1 the numbers of employees engaged in providing the Services;

1.6.2 the percentage of time spent by each employee engaged in providing the Services;

1.6.3 the extent to which each employee qualifies for membership of any of the Statutory Schemes or any Broadly Comparable scheme set up pursuant to the provisions of any of the Annexes to Part D (Pensions) (as appropriate); and

1.6.4 a description of the nature of the work undertaken by each employee by location.

1.7 The Supplier shall provide, and shall procure that each Subcontractor shall provide, all reasonable cooperation and assistance to the Buyer, any Replacement Supplier and/or any Replacement Subcontractor to ensure the smooth transfer of the Transferring Supplier Employees on the Service Transfer Date including providing sufficient information in advance of the Service Transfer Date to ensure that all necessary payroll arrangements can be made to enable the Transferring Supplier Employees to be paid as appropriate. Without prejudice to the generality of the foregoing, within 5 Working Days following the Service Transfer Date, the Supplier shall provide, and shall procure that each Subcontractor shall provide, to the Buyer or, at the direction of the Buyer, to any Replacement Supplier and/or any Replacement Subcontractor (as appropriate), in respect of each person on the Supplier's Final Supplier Personnel List who is a Transferring Supplier Employee:

1.7.1 the most recent month's copy pay slip data;

1.7.2 details of cumulative pay for tax and pension purposes;

1.7.3 details of cumulative tax paid;

1.7.4 tax code;

1.7.5 details of any voluntary deductions from pay; and

1.7.6 bank/building society account details for payroll purposes.

## 2. Staff Transfer when the contract ends

2.1 The Buyer and the Supplier acknowledge that subsequent to the commencement of the provision of the Services, the identity of the provider of the Services (or any part of the Services) may change (whether as a result of termination or Partial Termination of the relevant Contract or otherwise) resulting in the Services being undertaken by a Replacement Supplier and/or a Replacement Subcontractor. Such change in the identity of the supplier of such services may constitute a Relevant Transfer to which the Employment Regulations and/or the Acquired Rights Directive will apply. The Buyer and the Supplier agree that, as a result of the operation of the Employment Regulations, where a Relevant Transfer occurs, the contracts of employment between the Supplier and the Transferring Supplier Employees (except in relation to any contract terms disapplied through operation of regulation 10(2) of the Employment Regulations) will have effect on and from the Service Transfer Date as if originally made between the Replacement Supplier and/or a Replacement Subcontractor (as the case may be) and each such Transferring Supplier Employee.

2.2 The Supplier shall, and shall procure that each Subcontractor shall, comply with all its obligations in respect of the Transferring Supplier Employees arising under the Employment Regulations in respect of the period up to (and including) the Service Transfer Date and shall perform and discharge, and procure that each Subcontractor shall perform and discharge, all its obligations in respect of all the Transferring Supplier Employees arising in respect of the period up to (and including) the Service Transfer Date

(including (without limit) the payment of all remuneration, benefits, entitlements, and outgoings, all wages, accrued but untaken holiday pay, bonuses, commissions, payments ofPAYE, national insurance contributions and pension contributions and all such sums due as a result of any Fair Deal Employees' participation in the Schemes which in any case are attributable in whole or in part to the period ending on (and including) the Service Transfer Date) and any necessary apportionments in respect of any periodic payments shall be made between: (i) the Supplier and/or the Subcontractor (as appropriate); and (ii) the Replacement Supplier and/or Replacement Subcontractor.

2.3 Subject to Paragraph 2.4, the Supplier shall indemnify the Buyer and/or the Replacement Supplier and/or any Replacement Subcontractor against any Employee Liabilities arising from or as a result of:

2.3.1 any act or omission of the Supplier or any Subcontractor in respect of any Transferring Supplier Employee or any appropriate employee representative (as defined in the Employment Regulations) of any Transferring Supplier Employee whether occurring before, on or after the Service Transfer Date;

2.3.2 the breach or non-observance by the Supplier or any Subcontractor occurring on or before the Service Transfer Date of:

**(a) any collective agreement applicable to the Transferring Supplier Employees; and/or**

**(b) any other custom or practice with a trade union or staff association in respect of any Transferring Supplier Employees which the Supplier or any Subcontractor is contractually bound to honour;**

2.3.3 any claim by any trade union or other body or person representing any Transferring Supplier Employees arising from or connected with any failure by the Supplier or a Subcontractor to comply with any legal obligation to such trade union, body or person arising on or before the Service Transfer Date;

2.3.4 any proceeding, claim or demand by HMRC or other statutory authority in respect of any financial obligation including, but not limited to, PAYE and primary and secondary national insurance contributions:

**(a) in relation to any Transferring Supplier Employee, to the extent that the proceeding, claim or demand by HMRC or other statutory authority relates to financial obligations arising on and before the Service Transfer Date; and**

**(b) in relation to any employee who is not identified in the Supplier's Final Supplier Personnel List, and in respect of whom it is later alleged or determined that the Employment Regulations applied so as to transfer his/her employment from the Supplier to the Buyer and/or Replacement Supplier and/or any Replacement Subcontractor, to the extent that the proceeding, claim or demand by HMRC or other statutory authority relates to financial obligations arising on or before the Service Transfer Date;**

2.3.5 a failure of the Supplier or any Subcontractor to discharge or procure the discharge of all wages, salaries and all other benefits and all PAYE tax deductions and national insurance contributions relating to the Transferring Supplier Employees in respect of the period up to (and including) the Service Transfer Date);

2.3.6 any claim made by or in respect of any person employed or formerly employed by the Supplier or any Subcontractor other than a Transferring Supplier Employee identified in the Supplier's Final Supplier Personnel List for whom it is alleged the Buyer and/or the Replacement Supplier and/or any Replacement Subcontractor may be liable by virtue of the relevant Contract and/or the Employment Regulations and/or the Acquired Rights Directive; and

2.3.7 any claim made by or in respect of a Transferring Supplier Employee or any appropriate employee representative (as defined in the Employment Regulations) of any Transferring Supplier Employee relating to any act or omission of the Supplier or any Subcontractor in relation to its obligations under regulation 13 of the Employment Regulations, except to the extent that the liability arises from the failure by the Buyer and/or Replacement Supplier to comply with regulation 13(4) of the Employment Regulations.

2.4 The indemnities in Paragraph 2.3 shall not apply to the extent that the Employee Liabilities arise or are attributable to an act or omission of the Replacement Supplier and/or any Replacement Subcontractor whether

occurring or having its origin before, on or after the Service Transfer Date including any Employee Liabilities:

2.4.1 arising out of the resignation of any Transferring Supplier Employee before the Service Transfer Date on account of substantial detrimental changes to his/her working conditions proposed by the Replacement Supplier and/or any Replacement Subcontractor to occur in the period on or after the Service Transfer Date); or

2.4.2 arising from the Replacement Supplier's failure, and/or Replacement Subcontractor's failure, to comply with its obligations under the Employment Regulations.

2.5 If any person who is not identified in the Supplier's Final Supplier Employee List claims, or it is determined in relation to any employees of the Supplier, that his/her contract of employment has been transferred from the Supplier to the Replacement Supplier and/or Replacement Subcontractor pursuant to the Employment Regulations or the Acquired Rights Directive, then:

2.5.1 the Buyer shall procure that the Replacement Supplier and/or Replacement Subcontractor will, within 5 Working Days of becoming aware of that fact, notify the Buyer and the Supplier in writing; and

2.5.2 the Supplier may offer (or may procure that a Subcontractor may offer) employment to such person, or take such other reasonable steps as it considered appropriate to deal the matter provided always that such steps are in compliance with Law, within15 Working Days of receipt of notice from the Replacement Supplier and/or Replacement Subcontractor.

2.6 If such offer of is accepted, or if the situation has otherwise been resolved by the Supplier or a Subcontractor, Buyer shall procure that the Replacement Supplier shall, or procure that the and/or Replacement Subcontractor shall, immediately release or procure the release the person from his/her employment or alleged employment;

2.7 If after the 15 Working Day period specified in Paragraph 2.5.2 has elapsed:

2.7.1 no such offer has been made:

2.7.2 such offer has been made but not accepted; or

2.7.3 the situation has not otherwise been resolved

the Buyer shall advise the Replacement Supplier and/or Replacement Subcontractor (as appropriate) that it may within 5 Working Days give notice to terminate the employment or alleged employment of such person;

2.8 Subject to the Replacement Supplier's and/or Replacement Subcontractor acting in accordance with the provisions of Paragraphs 2.5 to 2.7 and in accordance with all applicable proper employment procedures set out in

applicable Law and subject to Paragraph 2.9 below, the Supplier will indemnify the Replacement Supplier and/or Replacement Subcontractor against all Employee Liabilities arising out of the termination of the employment of any of the Supplier's employees pursuant to the provisions of Paragraph 2.7 provided that the Replacement Supplier takes, or shall procure that the Replacement Subcontractor takes, all reasonable steps to minimise any such Employee Liabilities.

2.9 The indemnity in Paragraph 2.8:

2.9.1 shall not apply to:

(a) any claim for:

(i) discrimination, including on the grounds of sex, race, disability, age, gender reassignment, marriage or civil partnership, pregnancy and maternity or sexual orientation, religion or belief; or

(ii) equal pay or compensation for less favourable treatment of part-time workers or fixed-term employees,

In any case in relation to any alleged act or omission of the Replacement Supplier and/or Replacement Subcontractor, or

(b) any claim that the termination of employment was unfair because the Replacement Supplier and/or Replacement Subcontractor neglected to follow a fair dismissal procedure; and

2.9.2 shall apply only where the notification referred to in Paragraph 2.5.1 is made by the Replacement Supplier and/or Replacement Subcontractor to the Supplier within 6 months of the Service Transfer Date..

2.10 If any such person as is described in Paragraph 2.5 is neither re-employed by the Supplier or any Subcontractor nor dismissed by the Replacement Supplier and/or Replacement Subcontractor within the time scales set out in Paragraphs 2.5 to 2.7, such person shall be treated as a Transferring Supplier Employee. .

2.11 The Supplier shall comply, and shall procure that each Subcontractor shall comply, with all its obligations under the Employment Regulations and shall perform and discharge, and shall procure that each Subcontractor shall perform and discharge, all its obligations in respect of any person identified in the Supplier's Final Supplier Personnel List before and on the Service Transfer Date (including the payment of all remuneration, benefits, entitlements and outgoings, all wages, accrued but untaken holiday pay, bonuses, commissions, payments of PAYE, national insurance contributions and pension contributions and such sums due as a result of

any Fair Deal Employees' participation in the Schemes and any requirement to set up a broadly comparable pension scheme which in any case are attributable in whole or in part in respect of the period up to (and including) the Service Transfer Date) and any necessary apportionments in respect of any periodic payments shall be made between:

**(b) the Supplier and/or any Subcontractor; and**

**(c) the Replacement Supplier and/or the Replacement Subcontractor.**

2.12 The Supplier shall, and shall procure that each Subcontractor shall, promptly provide the Buyer and any Replacement Supplier and/or Replacement Subcontractor, in writing such information as is necessary to enable the Buyer, the Replacement Supplier and/or Replacement Subcontractor to carry out their respective duties under regulation 13 of the Employment Regulations. The Buyer shall procure that the Replacement Supplier and/or Replacement Subcontractor, shall promptly provide to the Supplier and each Subcontractor in writing such information as is necessary to enable the Supplier and each Subcontractor to carry out their respective duties under regulation 13 of the Employment Regulations.

2.13 Subject to Paragraph 2.14, the Buyer shall procure that the Replacement Supplier indemnifies the Supplier on its own behalf and on behalf of any Replacement Subcontractor and its Subcontractors against any Employee Liabilities arising from or as a result of:

2.13.1 any act or omission of the Replacement Supplier and/or Replacement Subcontractor in respect of any Transferring Supplier Employee in the Supplier's Final Supplier Personnel List or any appropriate employee representative (as defined in the Employment Regulations) of any such Transferring Supplier Employee;

2.13.2 the breach or non-observance by the Replacement Supplier and/or Replacement Subcontractor on or after the Service Transfer Date of:

**(a) any collective agreement applicable to the Transferring Supplier Employees identified in the Supplier's Final Supplier Personnel List; and/or**

**(b) any custom or practice in respect of any Transferring Supplier Employees identified in the Supplier's Final Supplier Personnel List which the Replacement Supplier and/or Replacement Subcontractor is contractually bound to honour;**

2.13.3 any claim by any trade union or other body or person representing any Transferring Supplier Employees identified in the Supplier's Final Supplier Personnel List arising from or connected with any failure by the Replacement Supplier and/or Replacement Subcontractor to comply with any legal obligation to such trade union, body or person arising on or after the Service Transfer Date;

2.13.4 any proposal by the Replacement Supplier and/or Replacement Subcontractor to change the terms and conditions of employment or working conditions of any Transferring Supplier Employees identified in the Supplier's Final Supplier Personnel List on or after their transfer to the Replacement Supplier or Replacement Subcontractor (as the case may be) on the Service Transfer Date, or to change the terms and conditions of employment or working conditions of any person identified in the Supplier's Final Supplier Personnel List who would have been a Transferring Supplier Employee but for their resignation (or decision to treat their employment as terminated under regulation 4(9) of the Employment Regulations) before the Service Transfer Date as a result of or for a reason connected to such proposed changes;

2.13.5 any statement communicated to or action undertaken by the Replacement Supplier or Replacement Subcontractor to, or in respect of, any Transferring Supplier Employee identified in the Supplier's Final Supplier Personnel List on or before the Service Transfer Date regarding the Relevant Transfer which has not been agreed in advance with the Supplier in writing;

2.13.6 any proceeding, claim or demand by HMRC or other statutory authority in respect of any financial obligation including, but not limited to, PAYE and primary and secondary national insurance contributions:

**(a) in relation to any Transferring Supplier Employee identified in the Supplier's Final Supplier Personnel List, to the extent that the proceeding, claim or demand by HMRC or other statutory authority relates to financial obligations arising after the Service Transfer Date; and**

**(b) in relation to any employee who is not a Transferring Supplier Employee identified in the Supplier's Final Supplier Personnel List, and in respect of whom it is later alleged or determined that the Employment Regulations applied so as to transfer his/her employment from the Supplier or Subcontractor, to the Replacement Supplier or Replacement Subcontractor to the extent that the proceeding, claim or demand by HMRC or other statutory authority relates to financial obligations arising after the Service Transfer Date;**

2.13.7 a failure of the Replacement Supplier or Replacement Subcontractor to discharge or procure the discharge of all wages, salaries and all other benefits and all PAYE tax deductions and national insurance contributions relating to the Transferring Supplier Employees identified in the Supplier's Final Supplier Personnel List in respect of the period from (and including) the Service Transfer Date; and

2.13.8 any claim made by or in respect of a Transferring Supplier Employee identified in the Supplier's Final Supplier Personnel List or any appropriate employee representative (as defined in the Employment Regulations) of any such Transferring Supplier Employee relating to any act or omission of the Replacement Supplier or Replacement Subcontractor in relation to obligations under regulation 13 of the Employment Regulations.

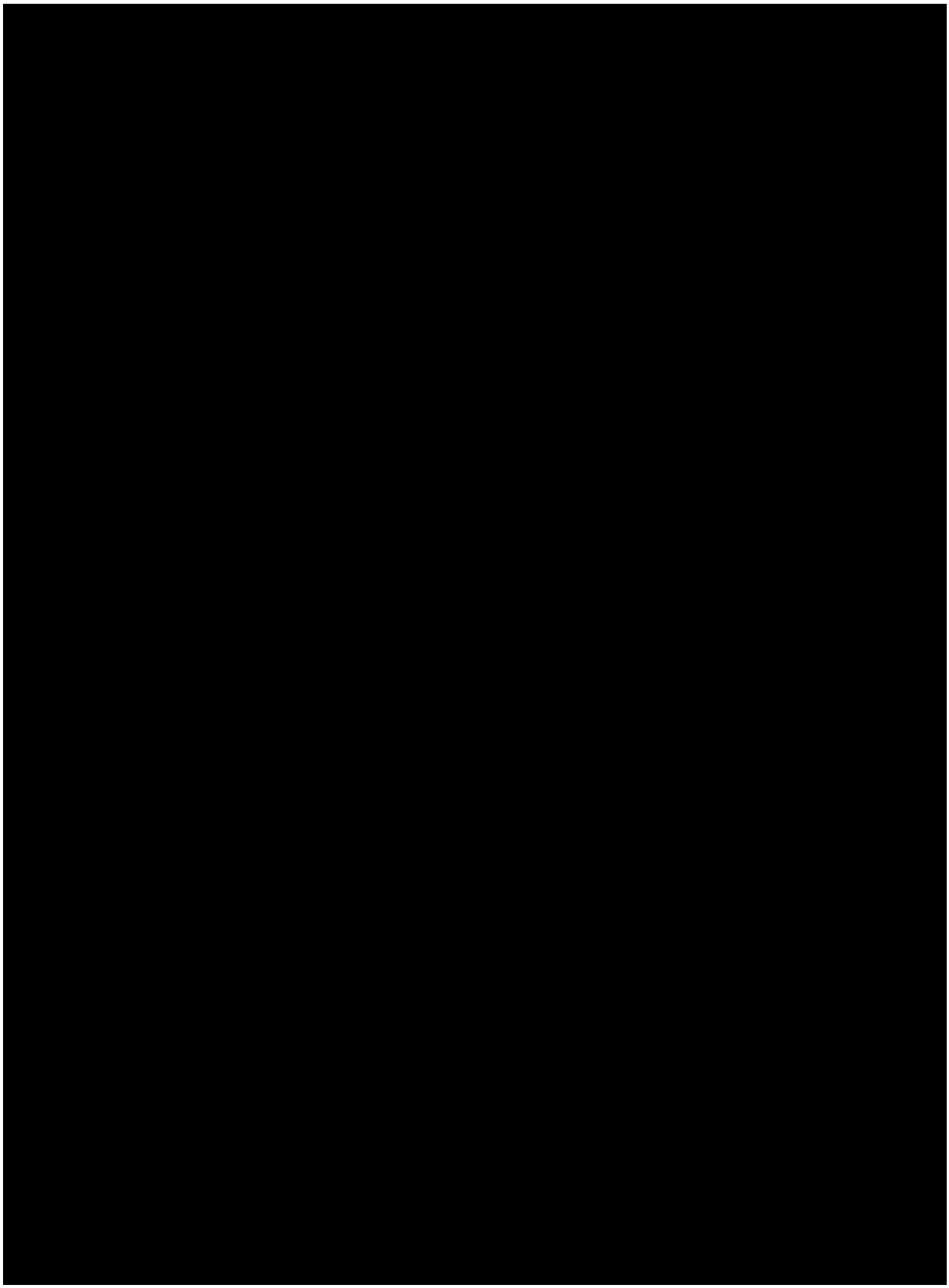
2.14 The indemnities in Paragraph 2.13 shall not apply to the extent that the Employee Liabilities arise or are attributable to an act or omission of the Supplier and/or any Subcontractor (as applicable) whether occurring or having its origin before, on or after the Service Transfer Date, including any Employee Liabilities arising from the failure by the Supplier and/or any Subcontractor (as applicable) to comply with its obligations under the Employment Regulations.

# Call-Off Schedule 4 (Call Off Tender)

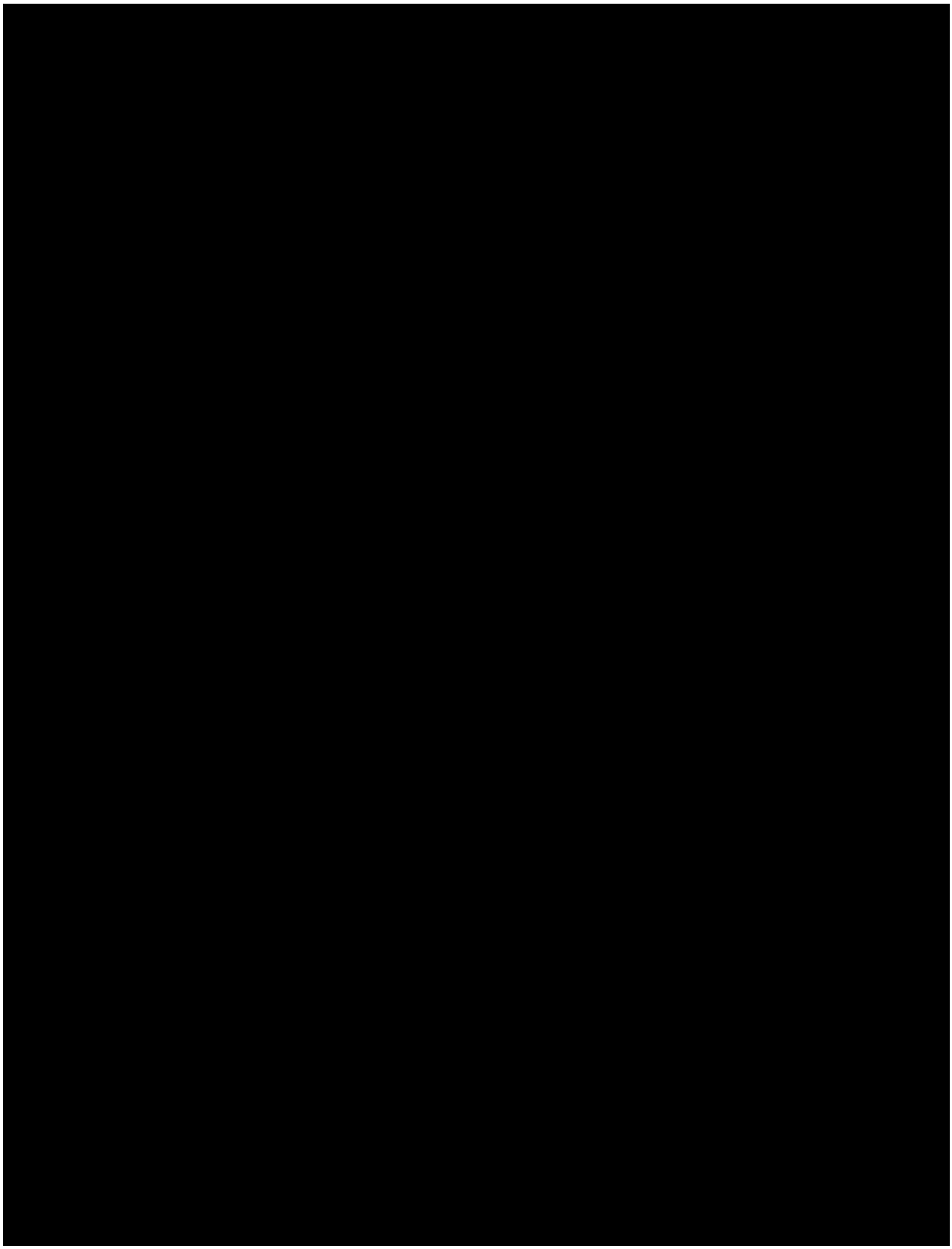

### 1. How will you ensure electronic and hard copy records are stored securely and preserved so as to avoid deterioration, corruption, damage or loss? Weighting 25%

*Your answer to each question must be no more than 4 pages A4 in length. Any answers over this length will be disregarded.*

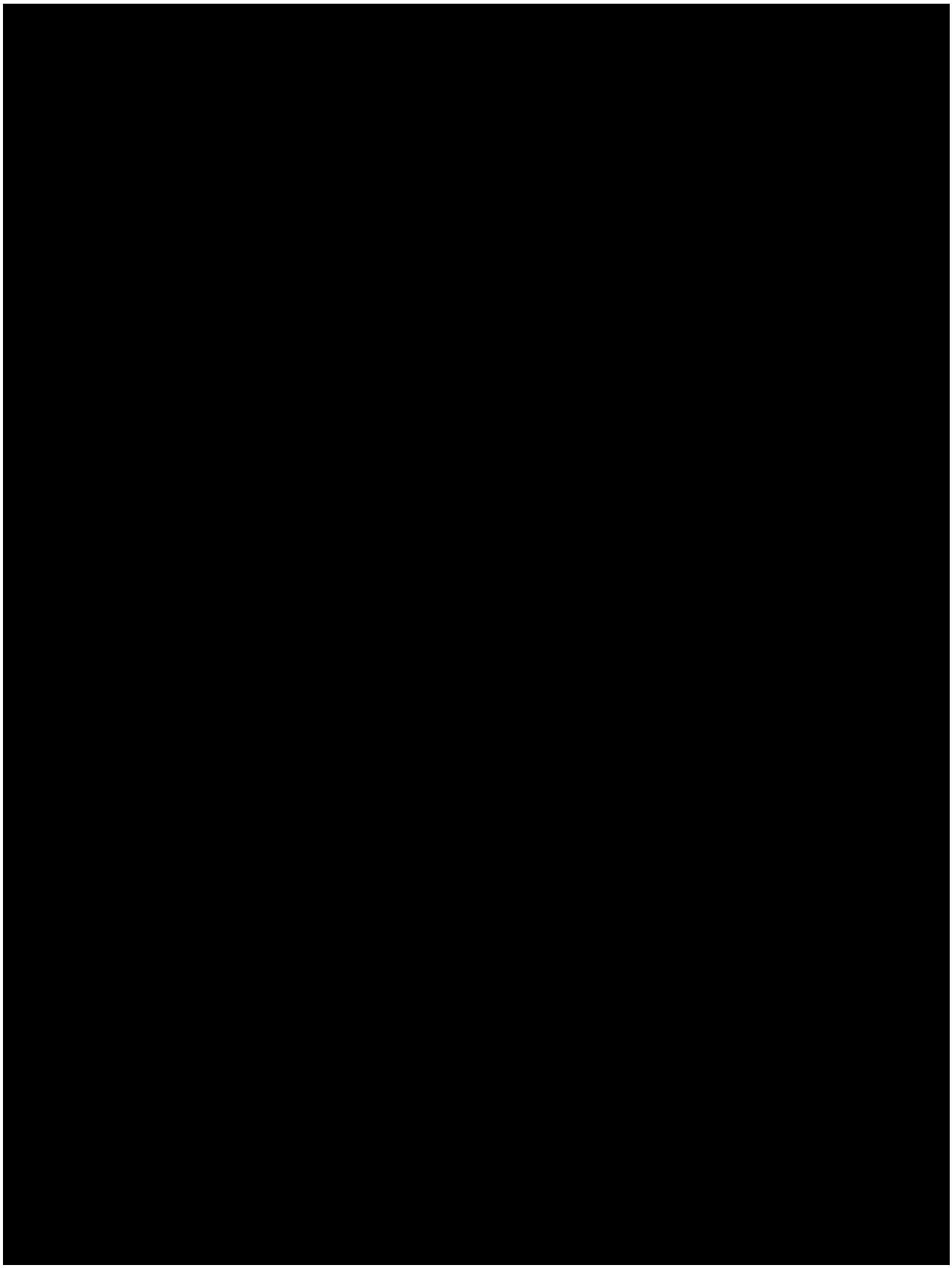
*Commercial in Confidence* *1*

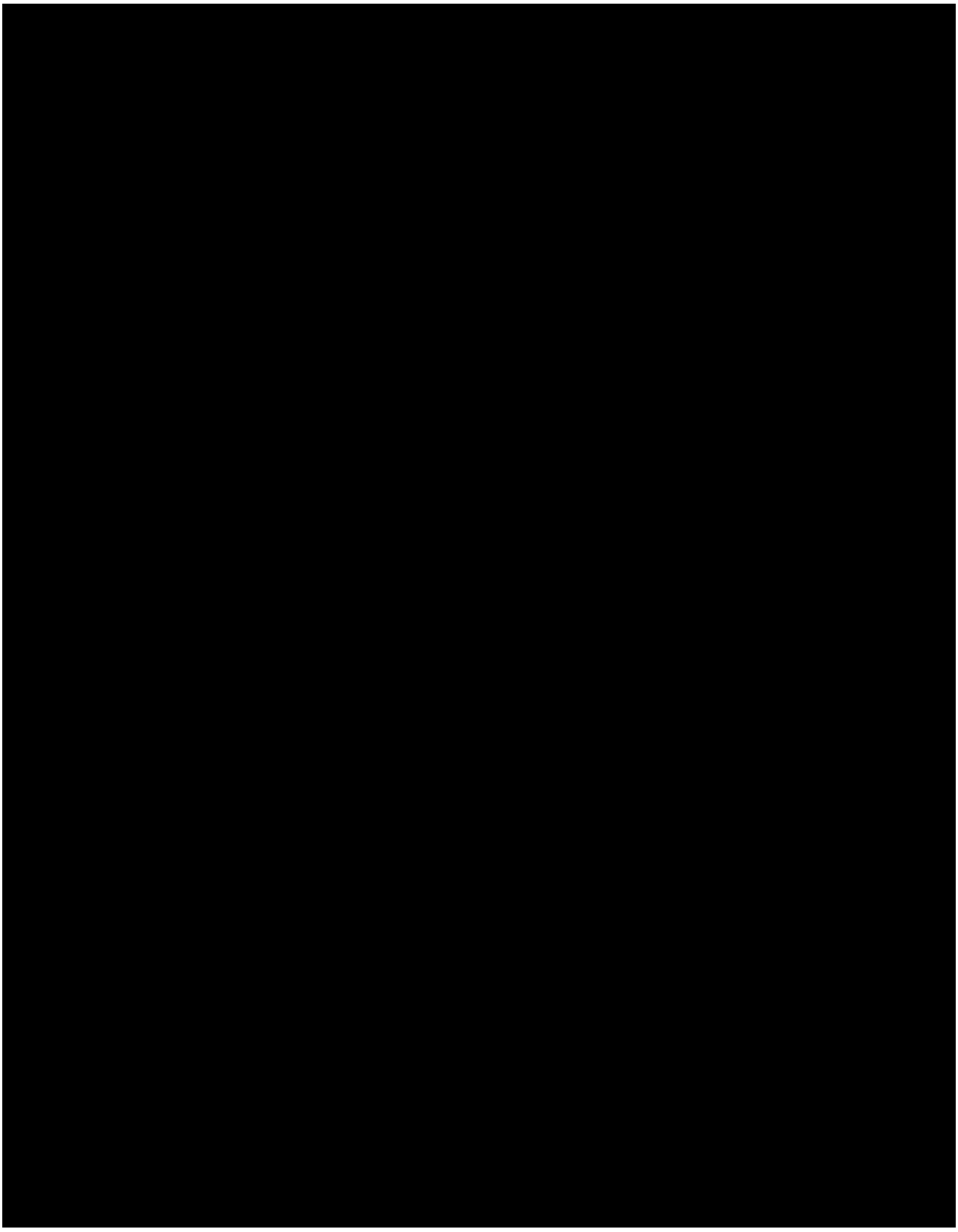


*Commercial in Confidence* *2*



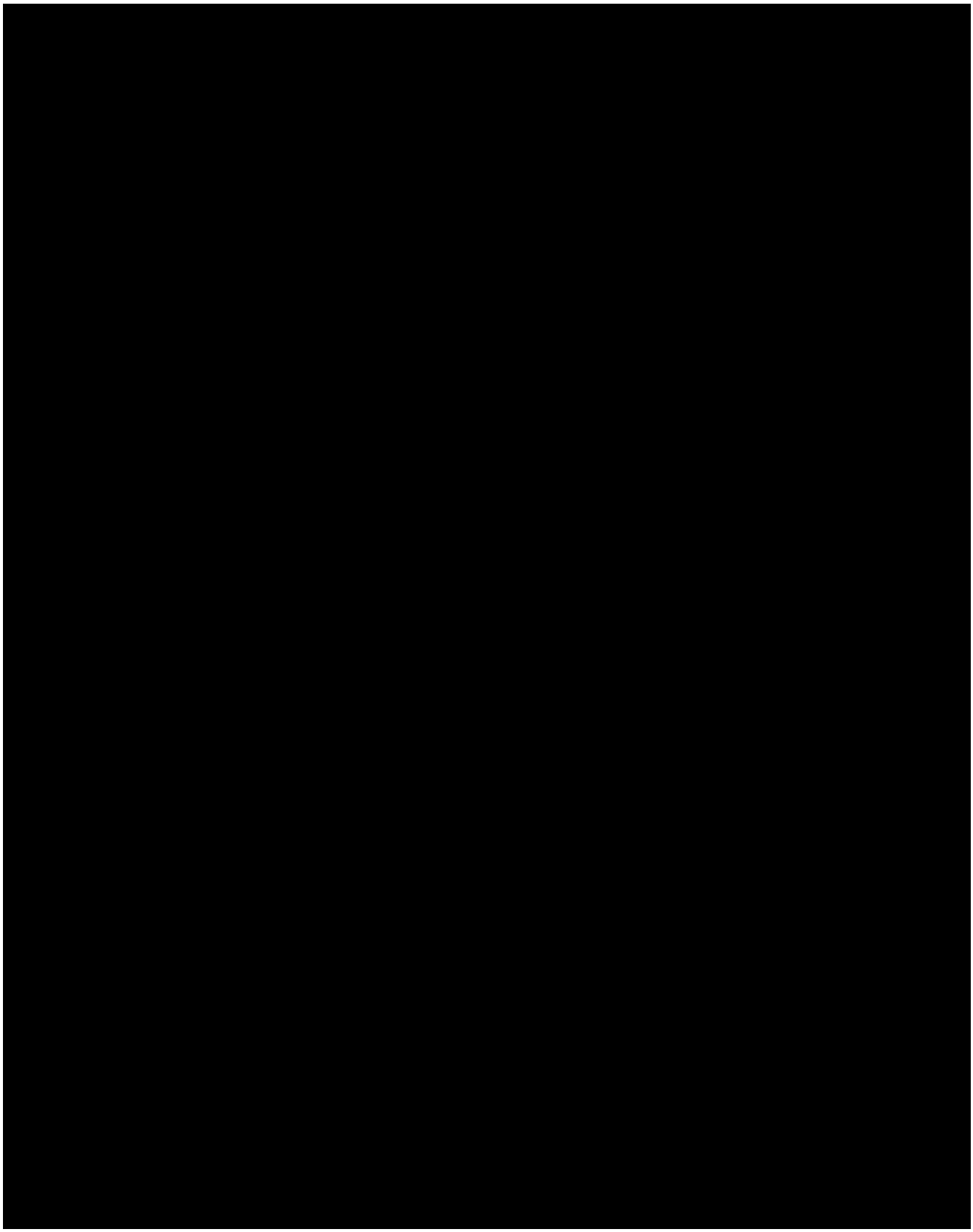
*Commercial in Confidence* *3*

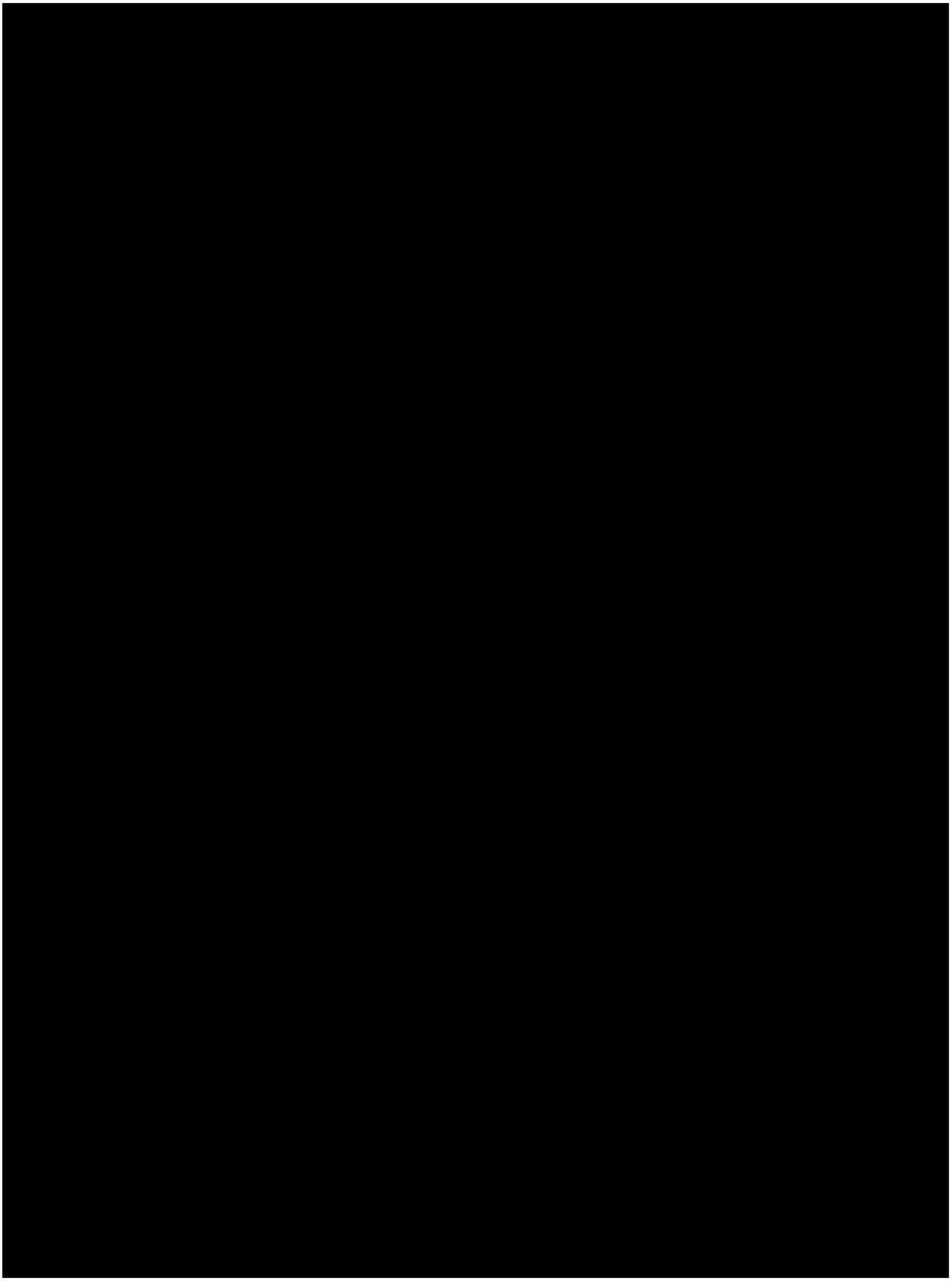


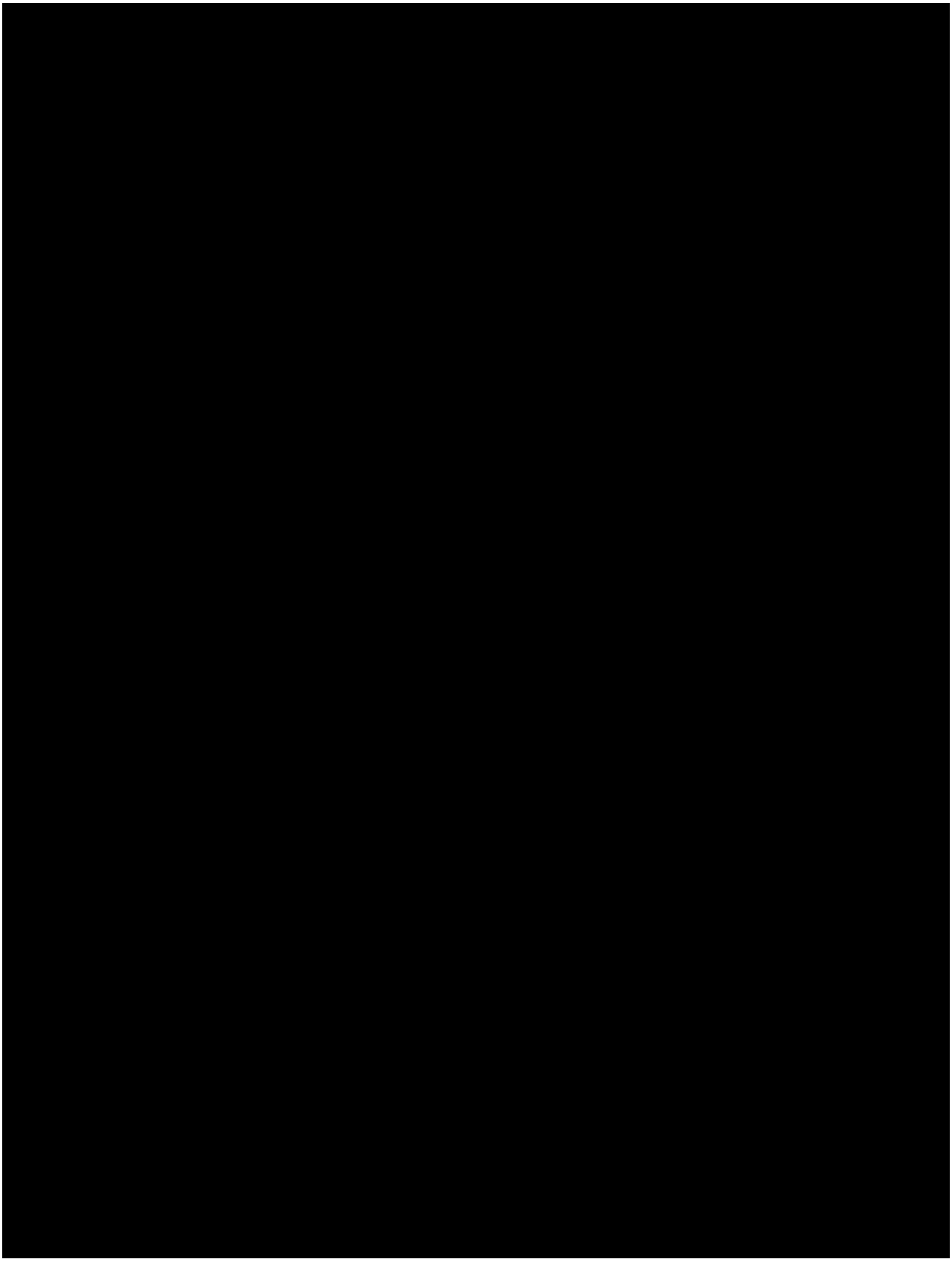


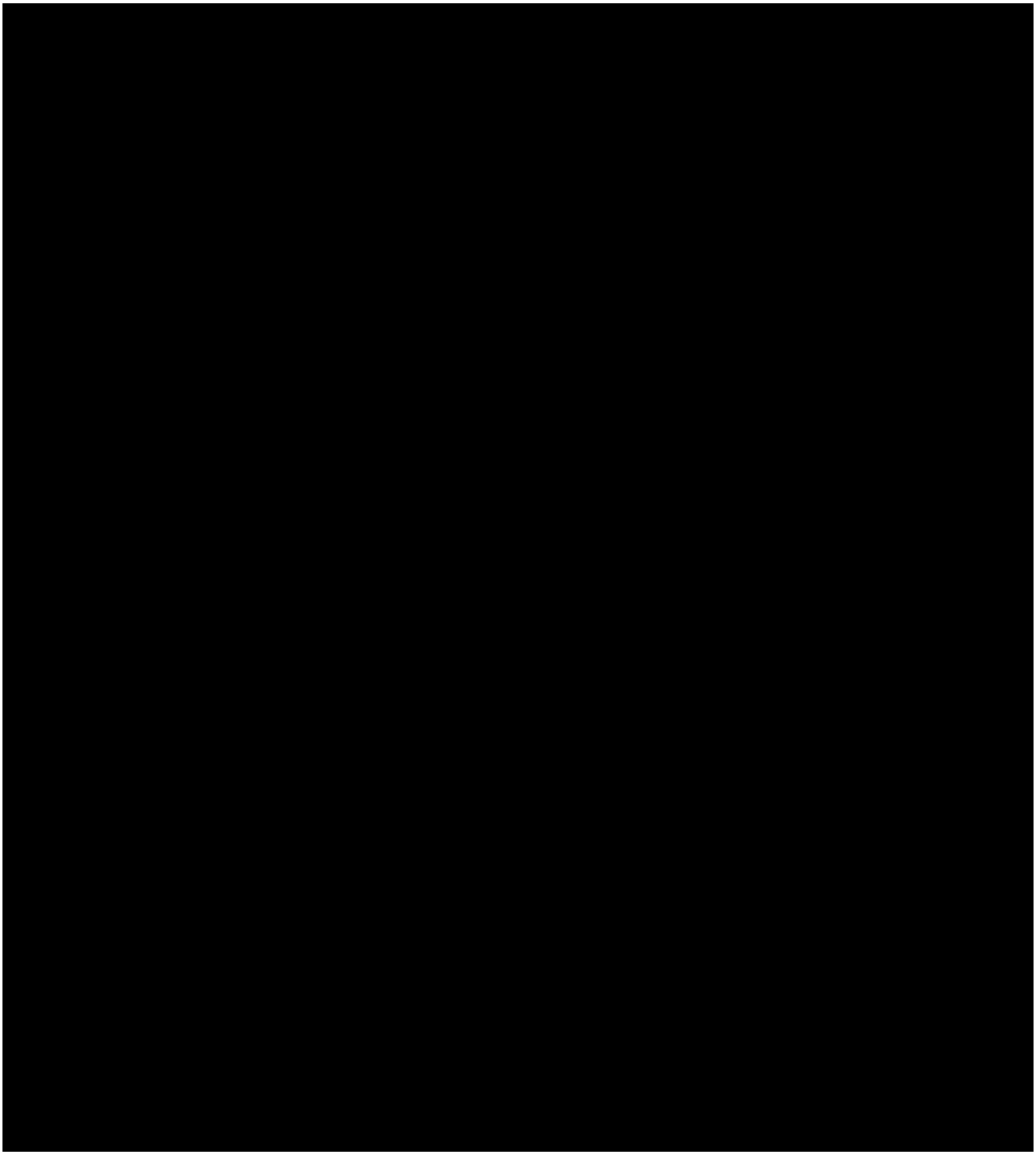

## Q2. How will you ensure that required response times for provision of data are met? Weighting 25%

*Your answer to each question must be no more than 4 pages A4 in length. Any answers over this length will be disregarded.*





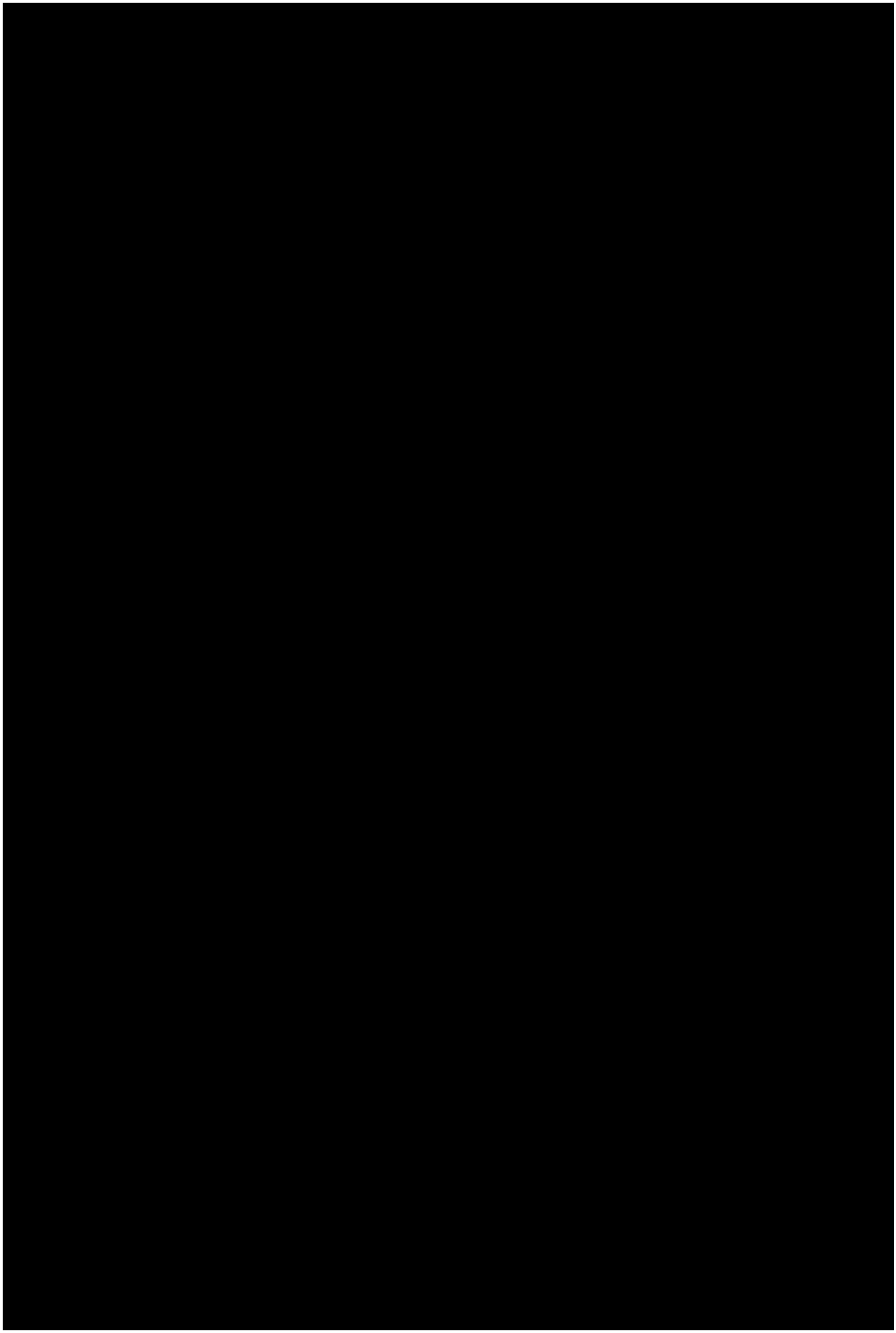


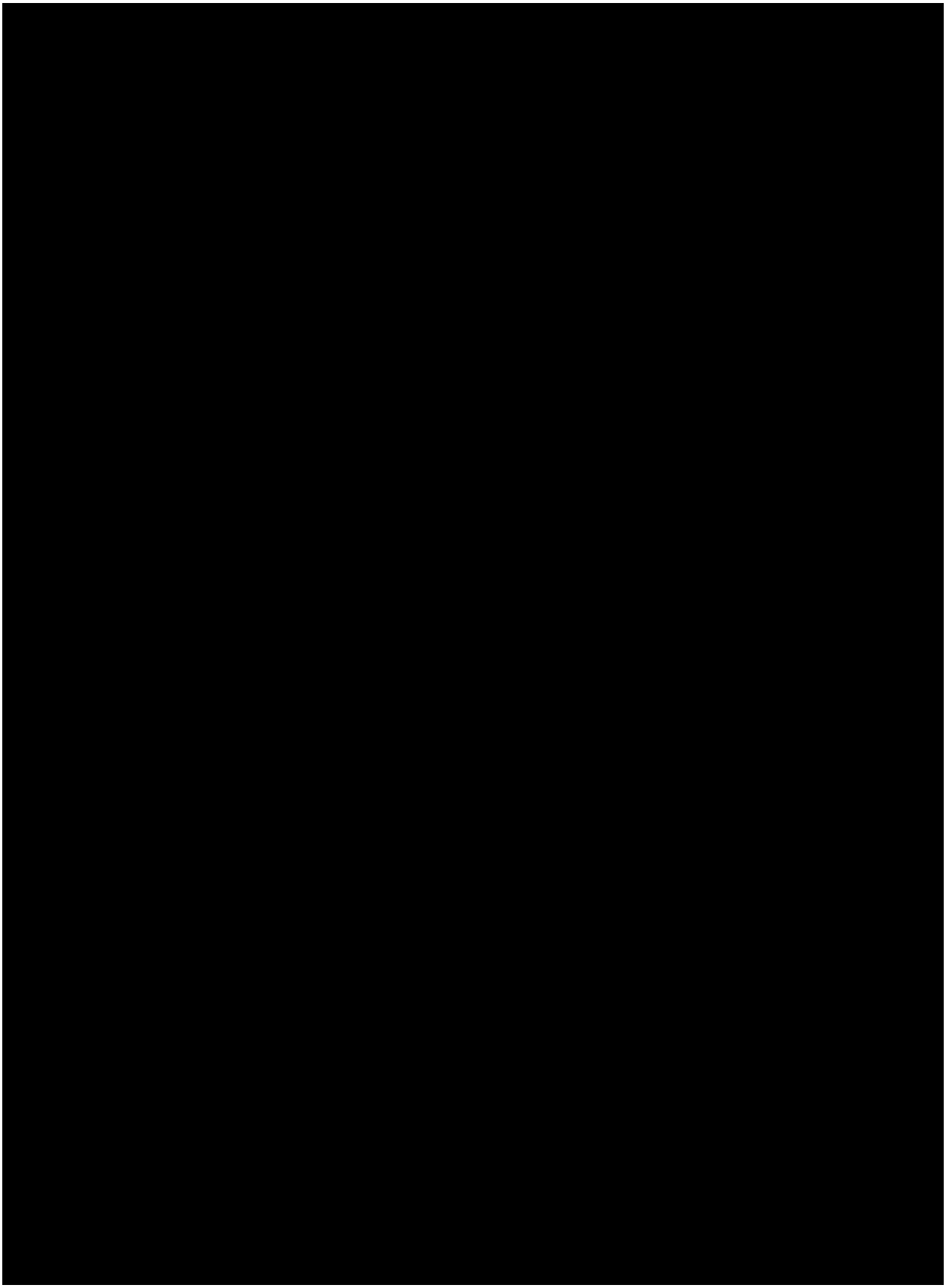


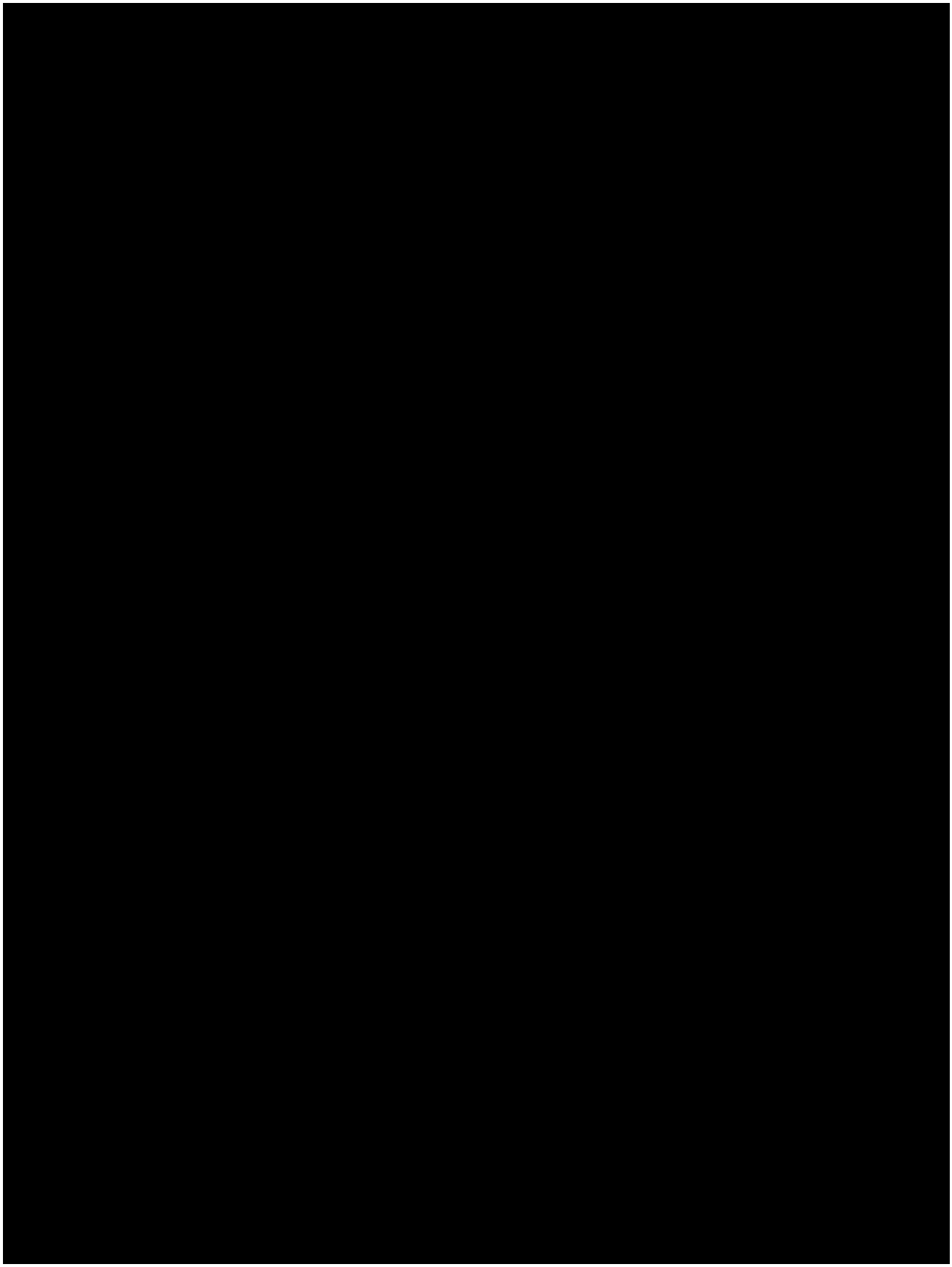
Commercial in
Confidence

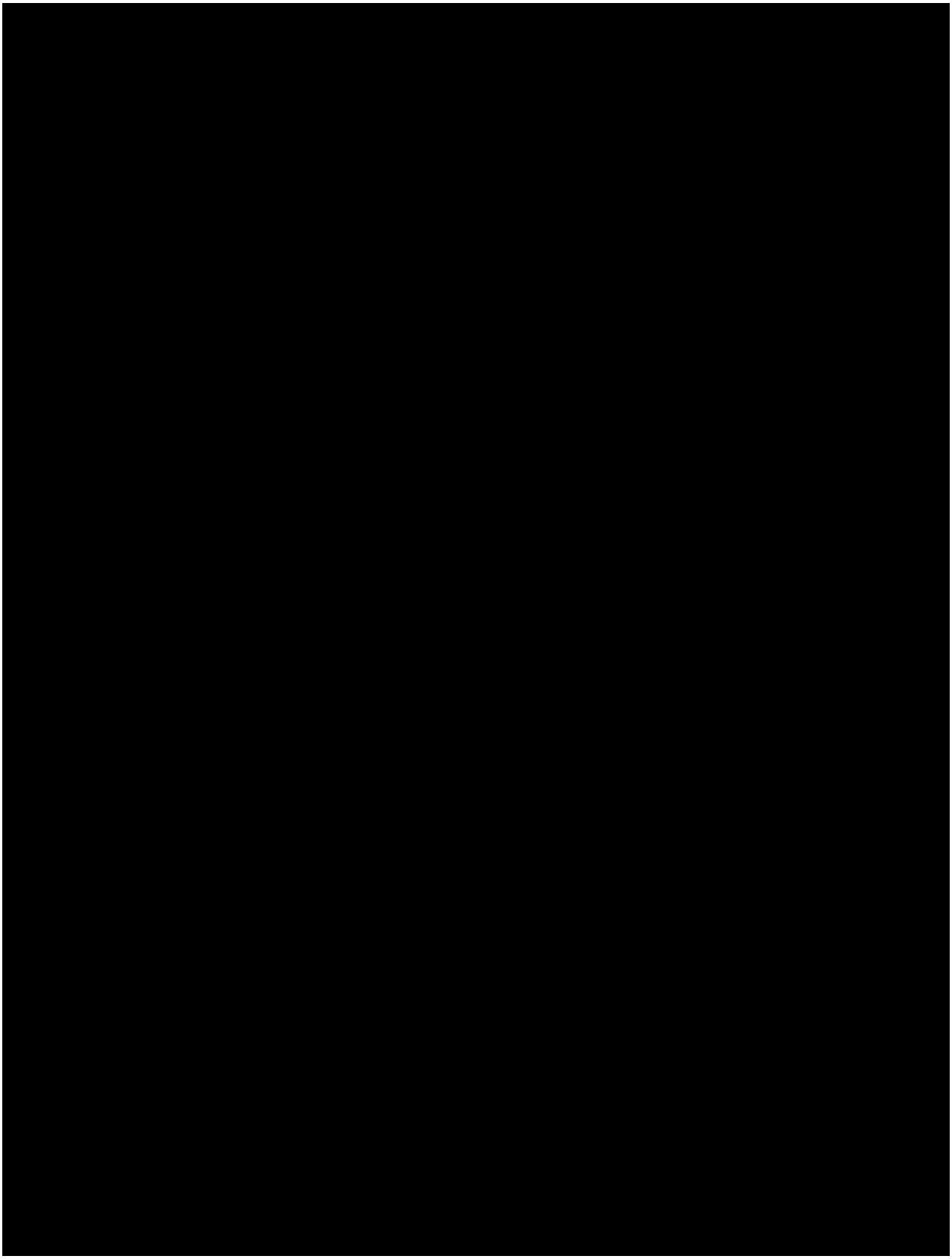

## Q3. How will you ensure that data is shared appropriately? Weighting 25%

*Your answer to each question must be no more than 4 pages A4 in length. Any answers over this length will be disregarded.*



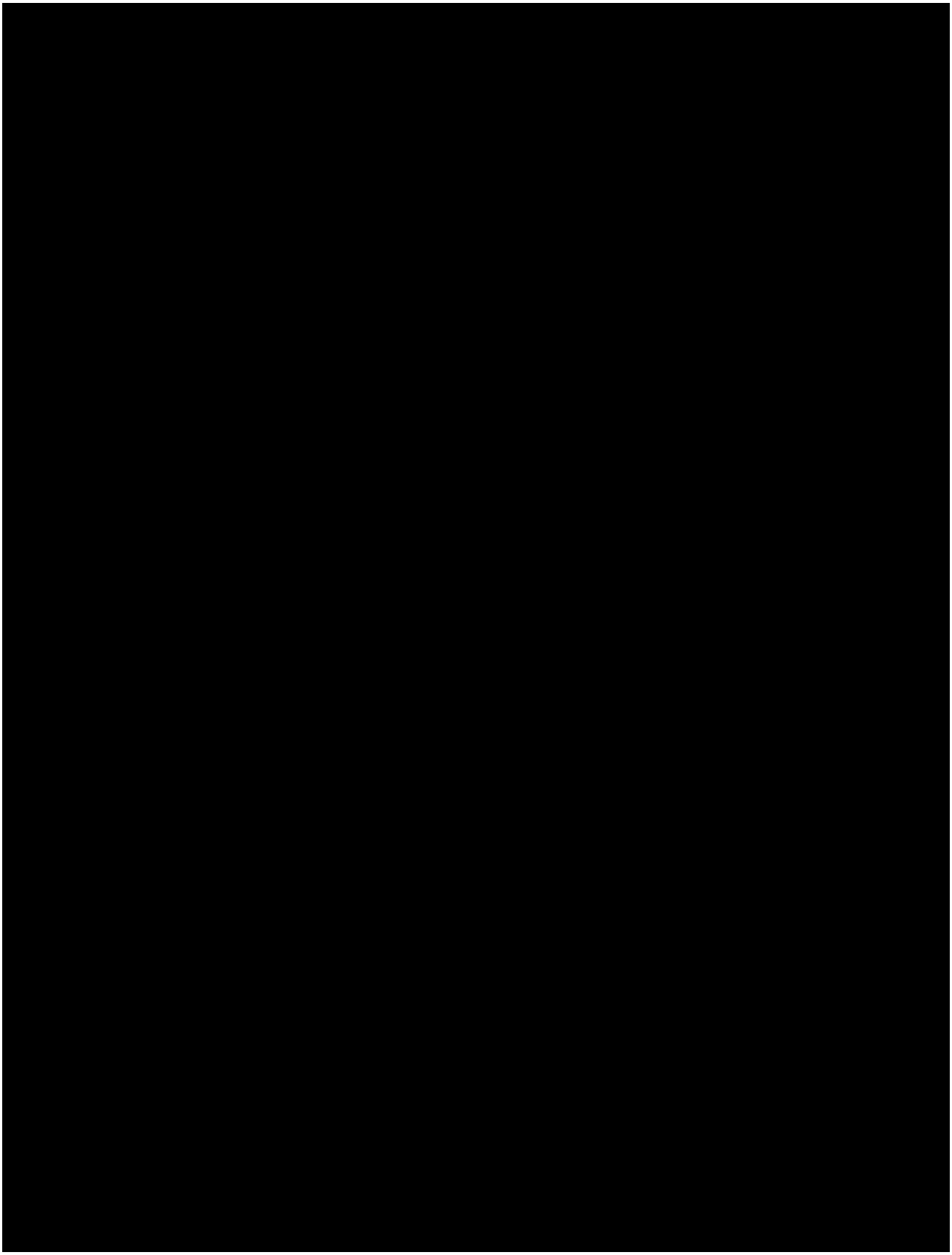


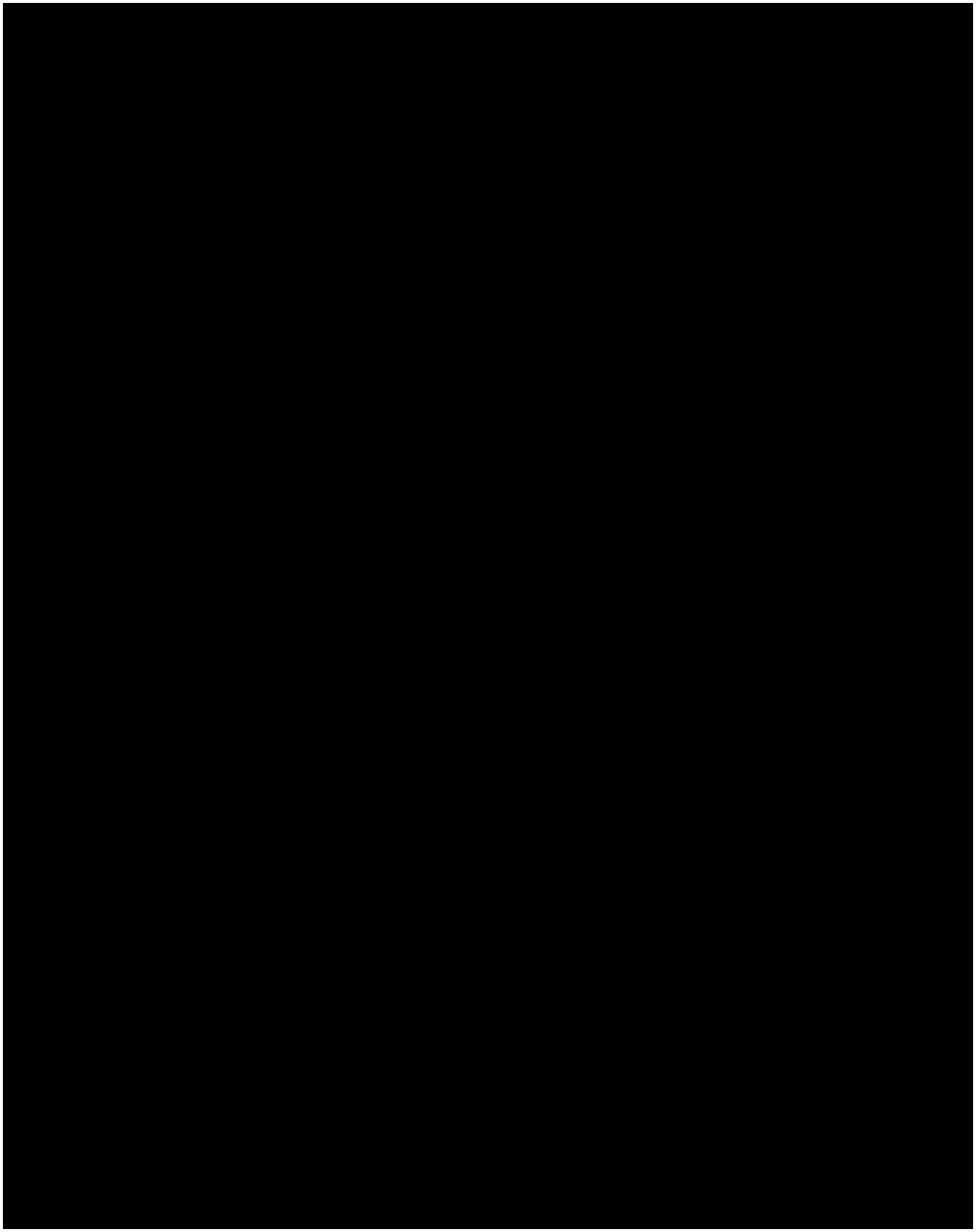


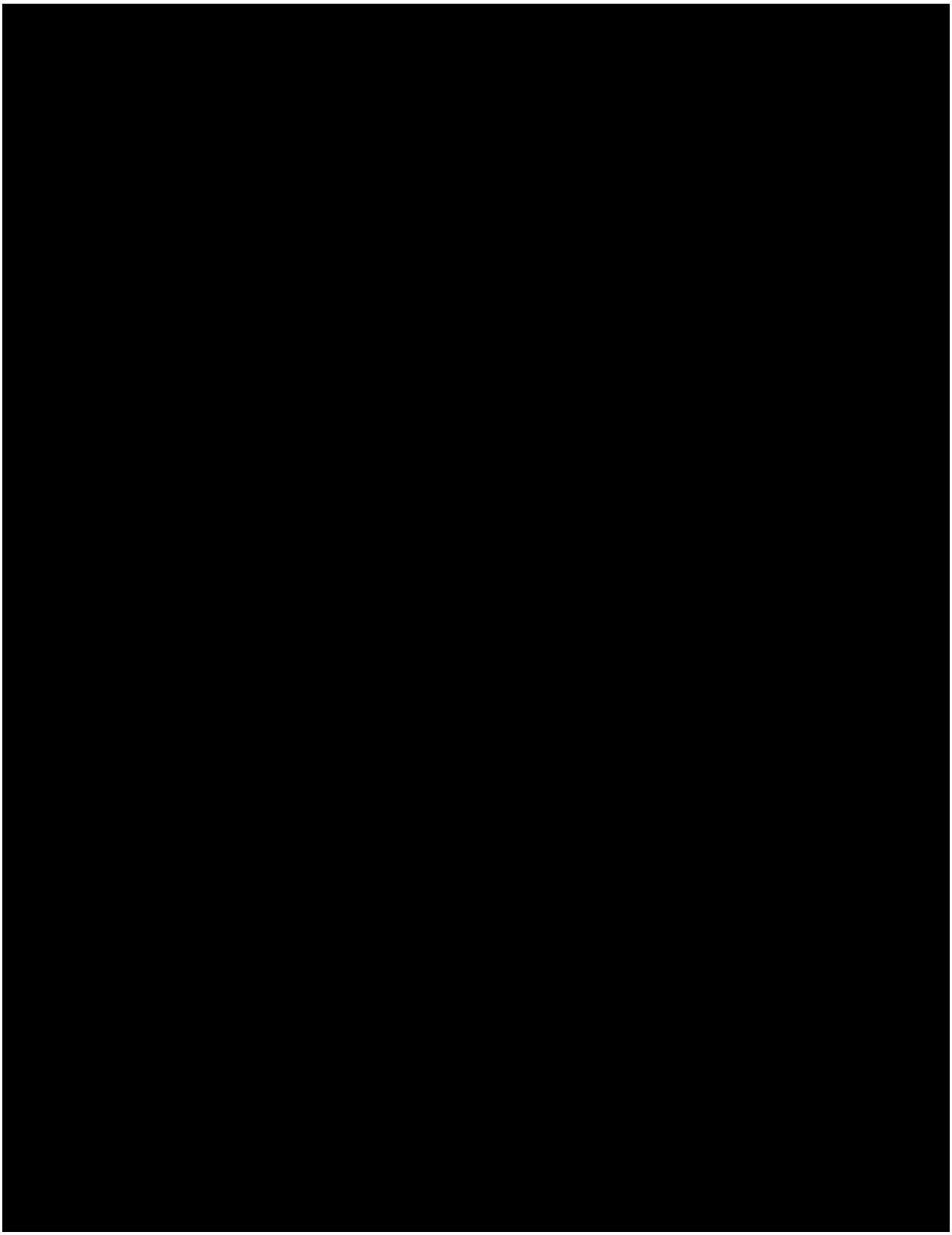


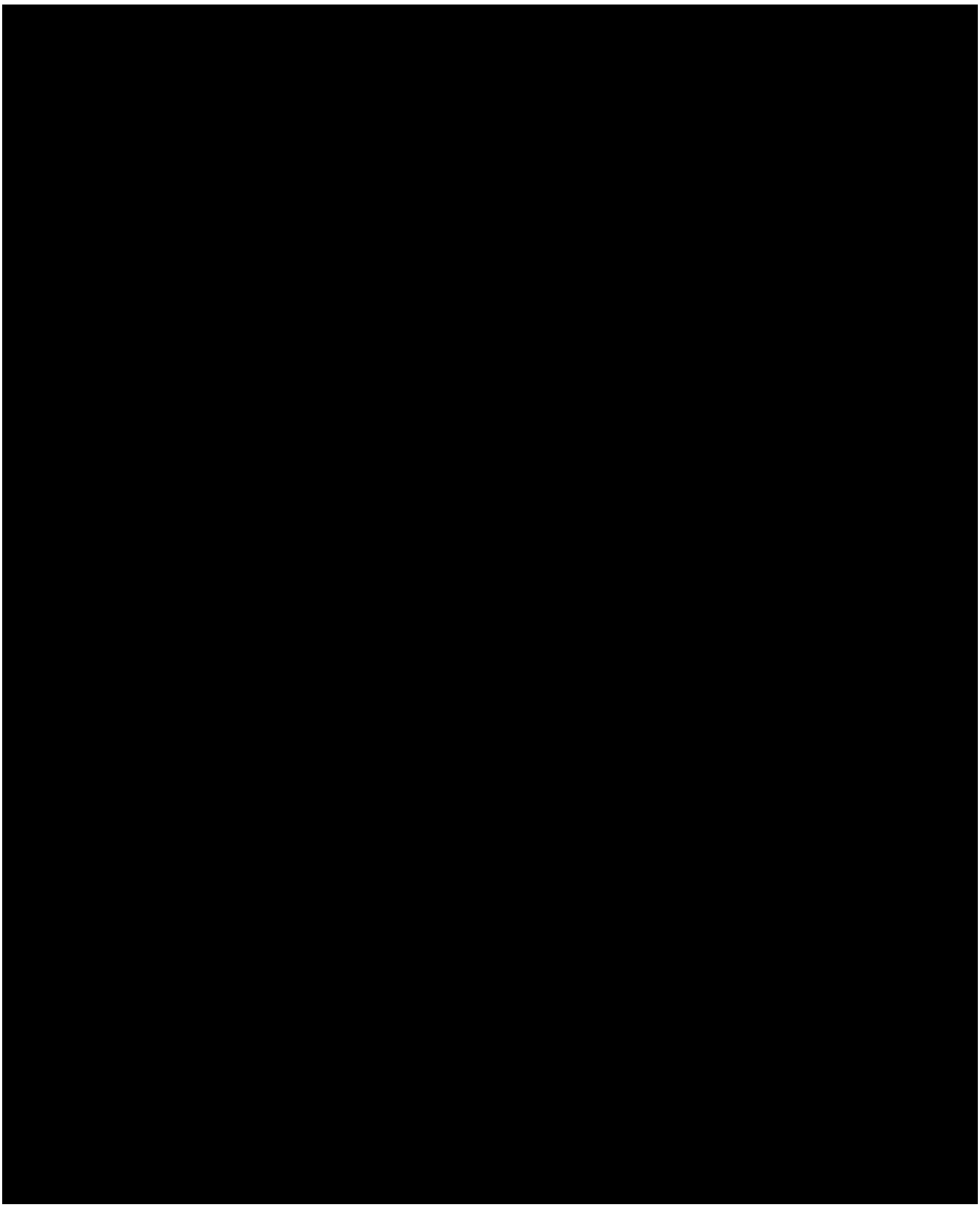

## Q4. How will you respond to any future change in requirements? Weighting 15%

*Your answer to each question must be no more than 4 pages A4 in length. Any answers over this length will be disregarded.*



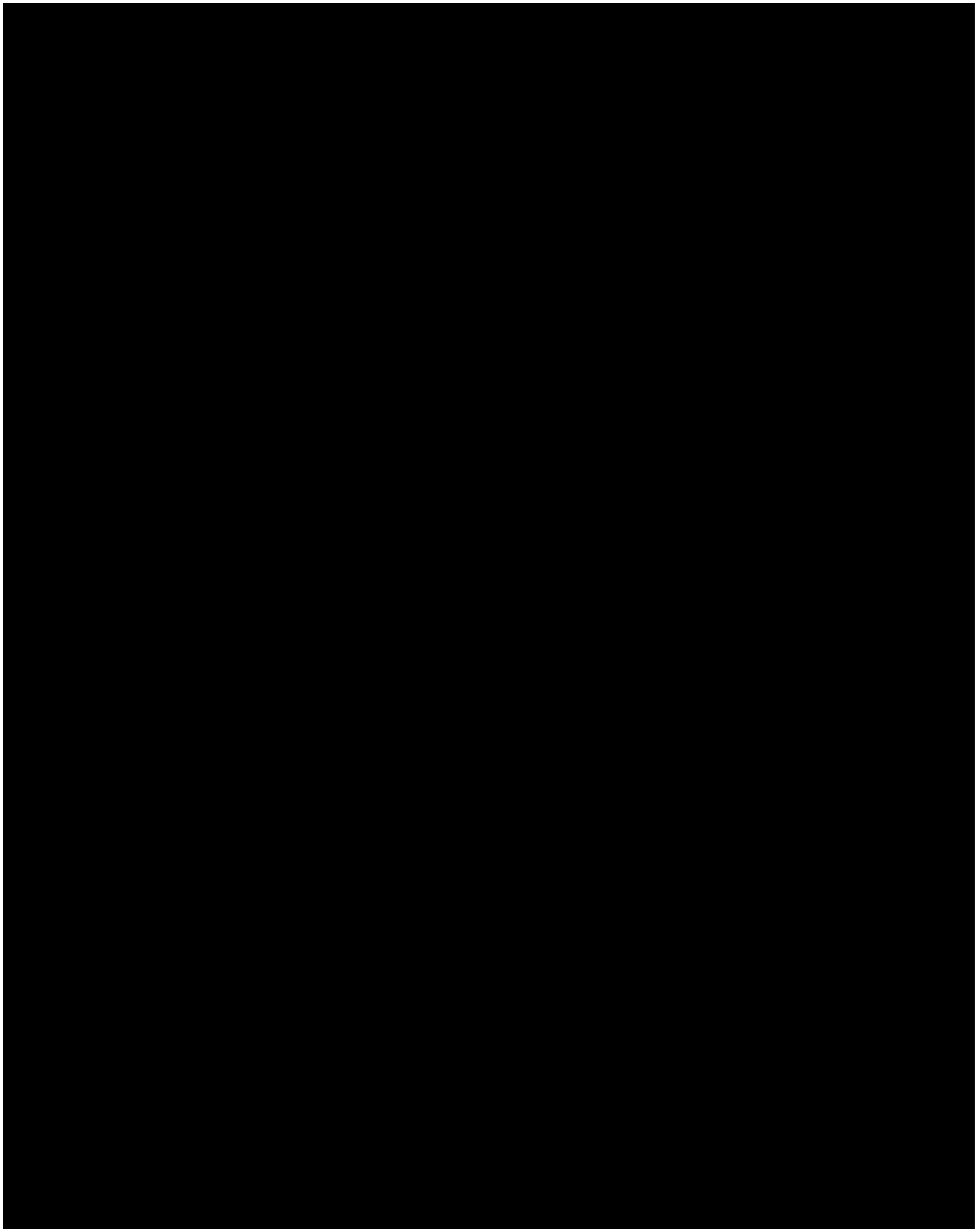


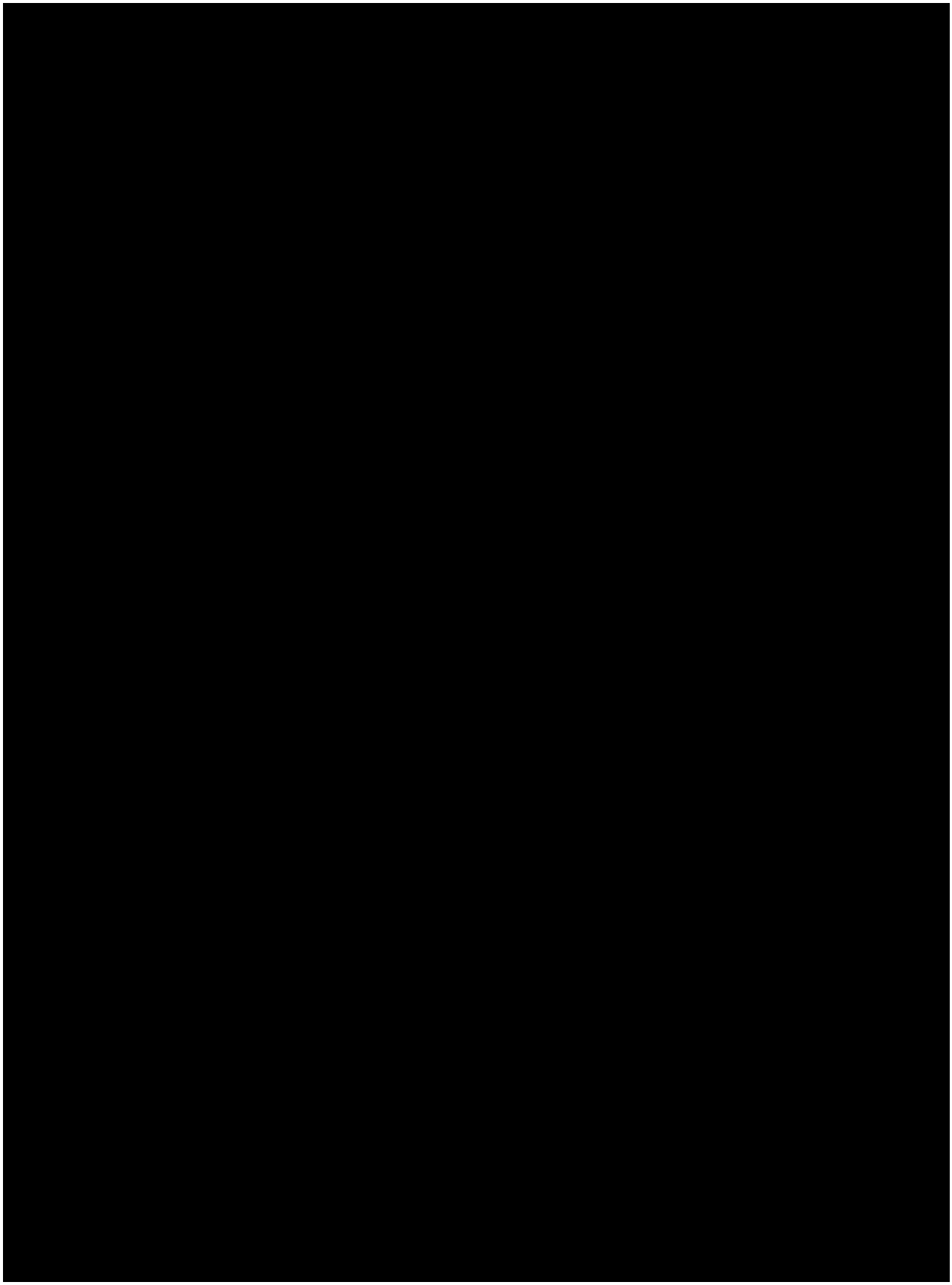


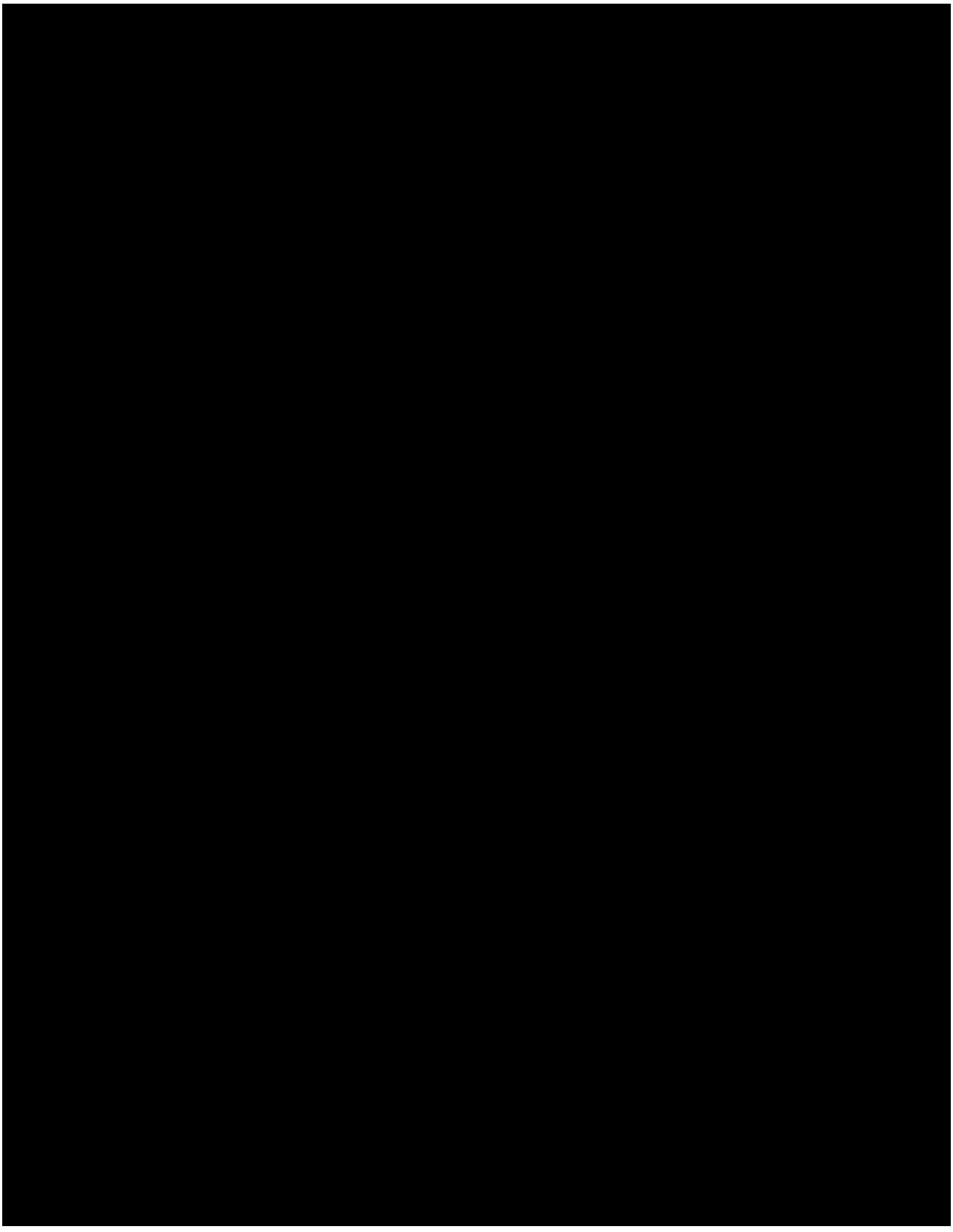


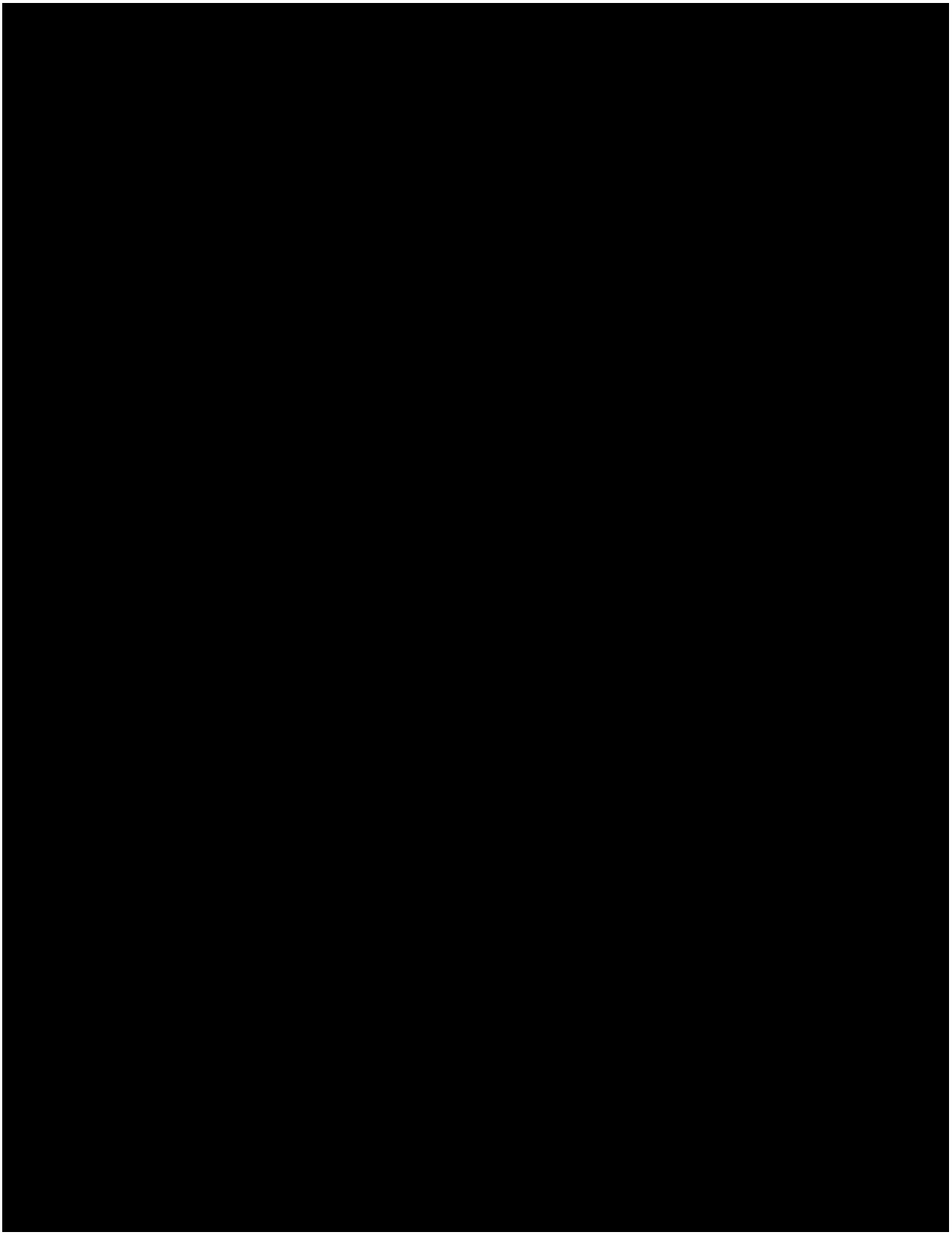

## Q5. How will ensure ongoing value for money? Weighting 10%

*Your answer to each question must be no more than 4 pages A4 in length. Any answers over this length will be disregarded.*





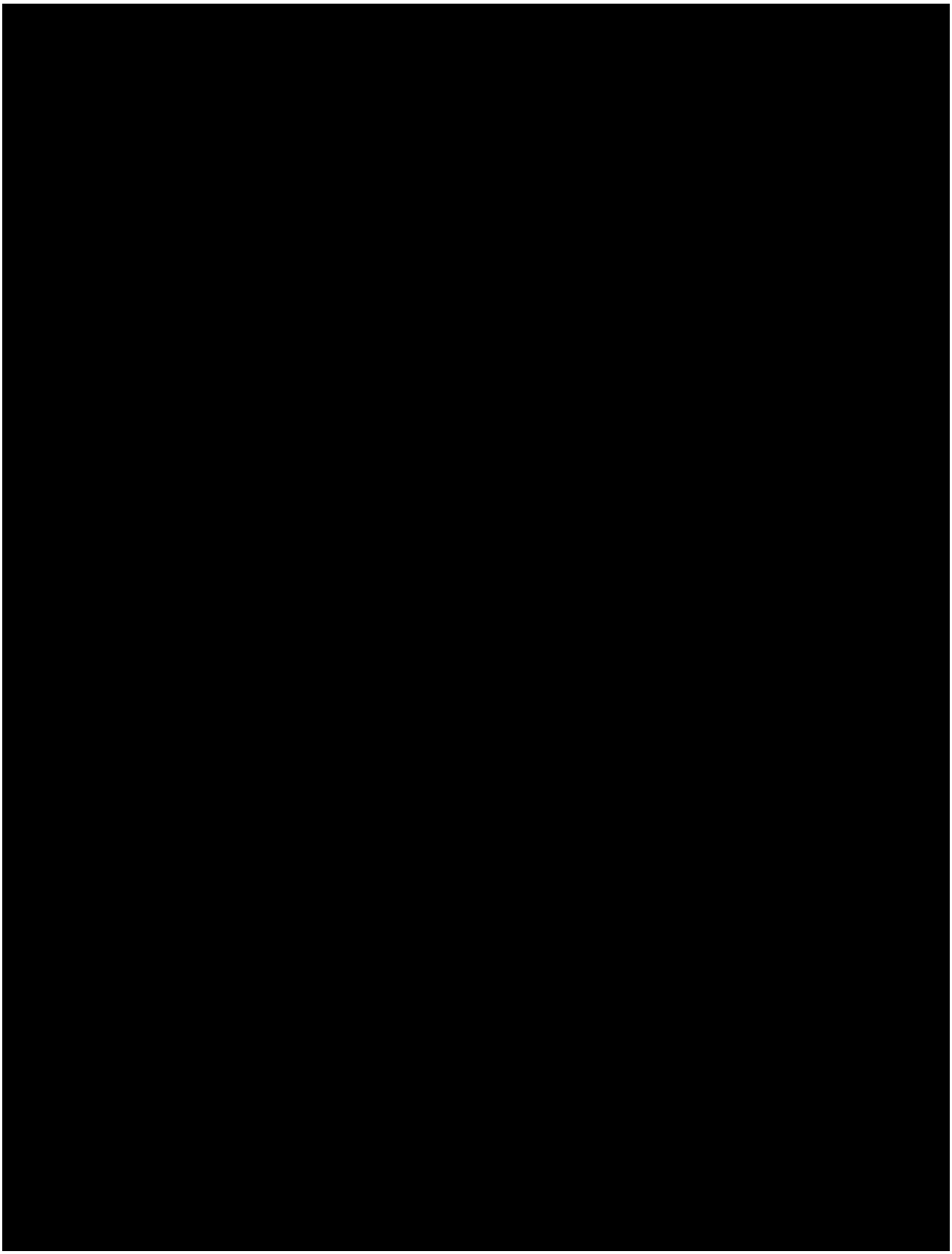


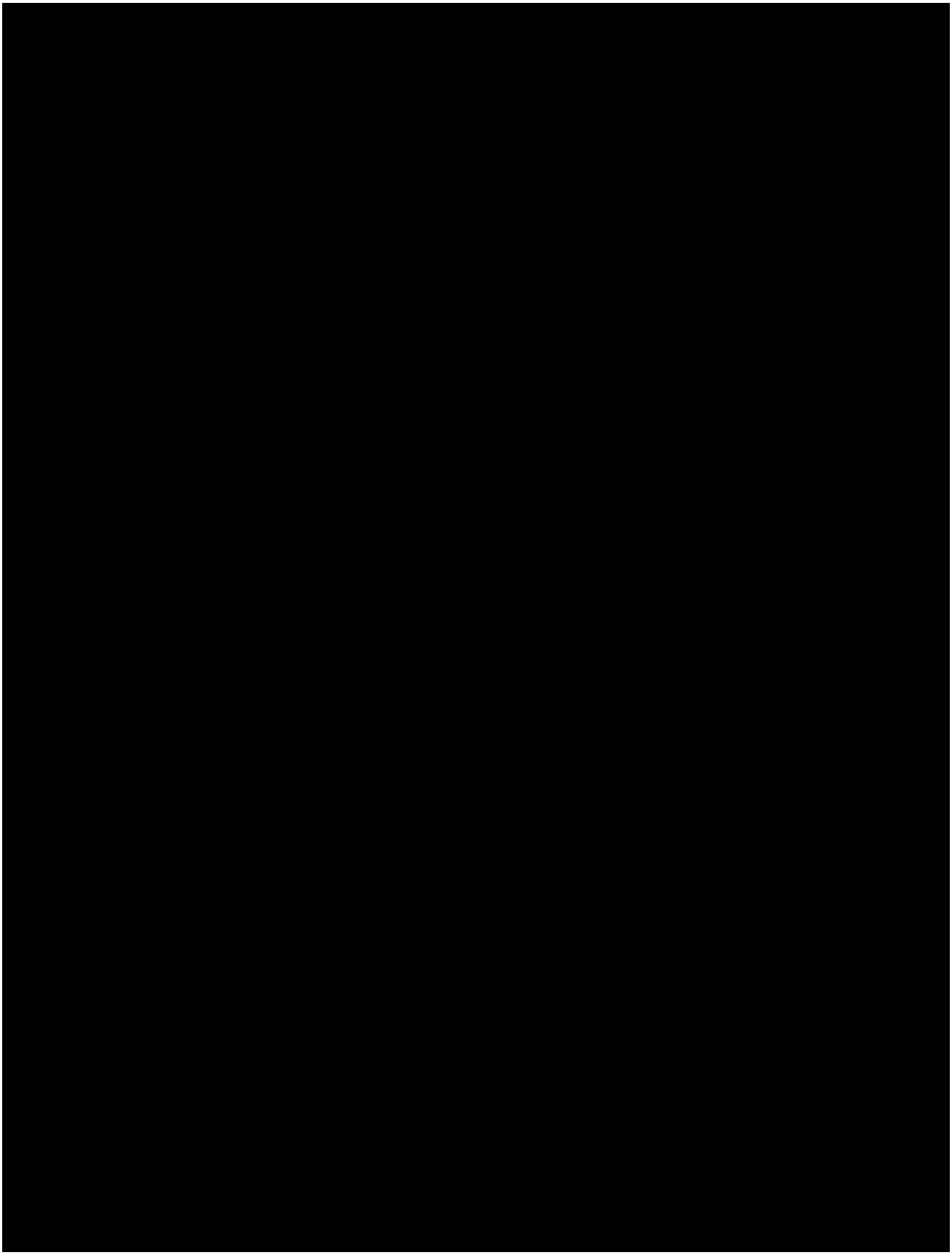


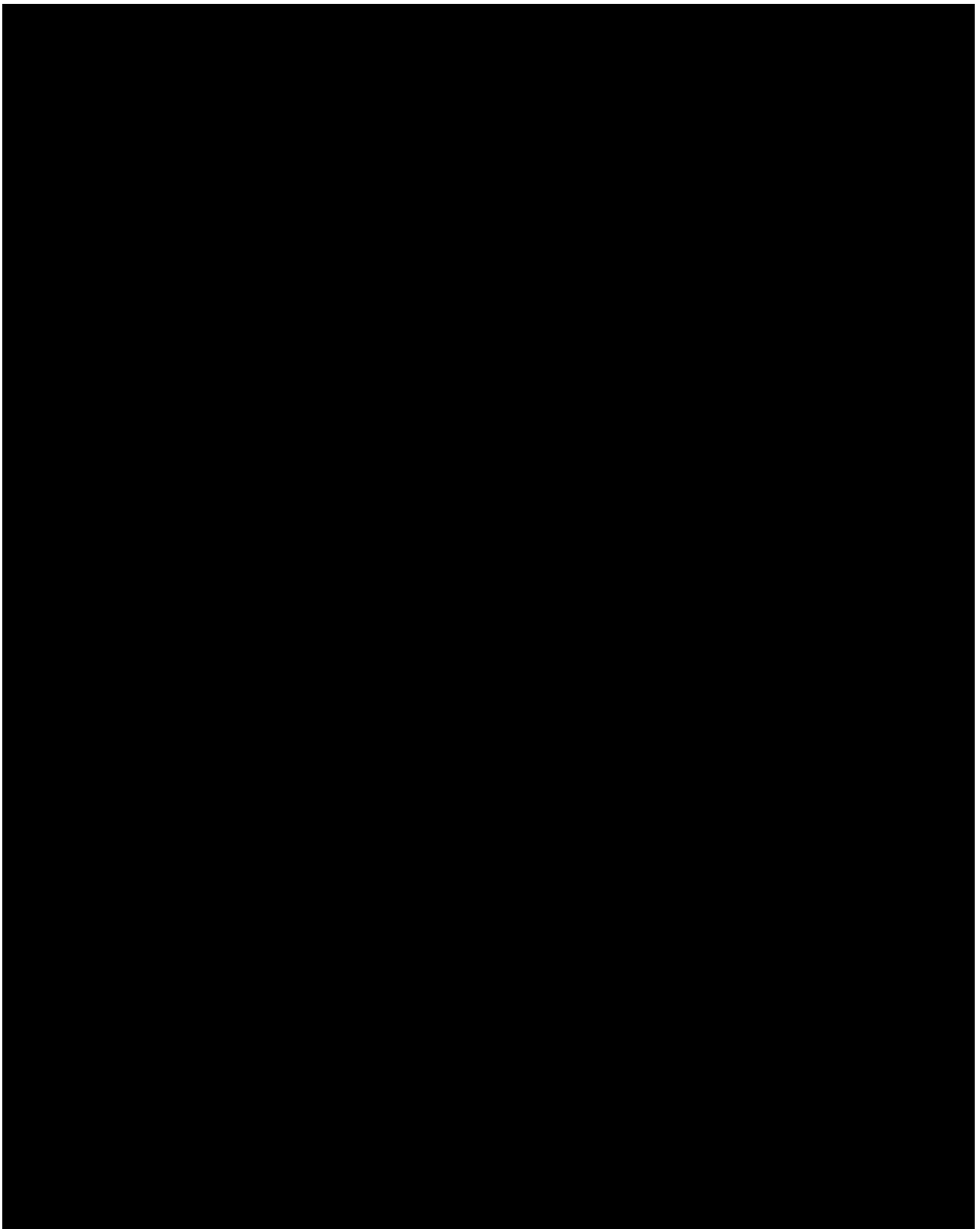

**Question: Describe the commitment your organisation will make to ensure that opportunities under the contract deliver the Policy Outcome and Award Criteria for MAC 4.1 - Deliver additional environmental benefits in the performance of the contract including working towards net zero greenhouse gas.**

**How will you support DESNZ mission to achieve Net Zero in the UK by 2050?**

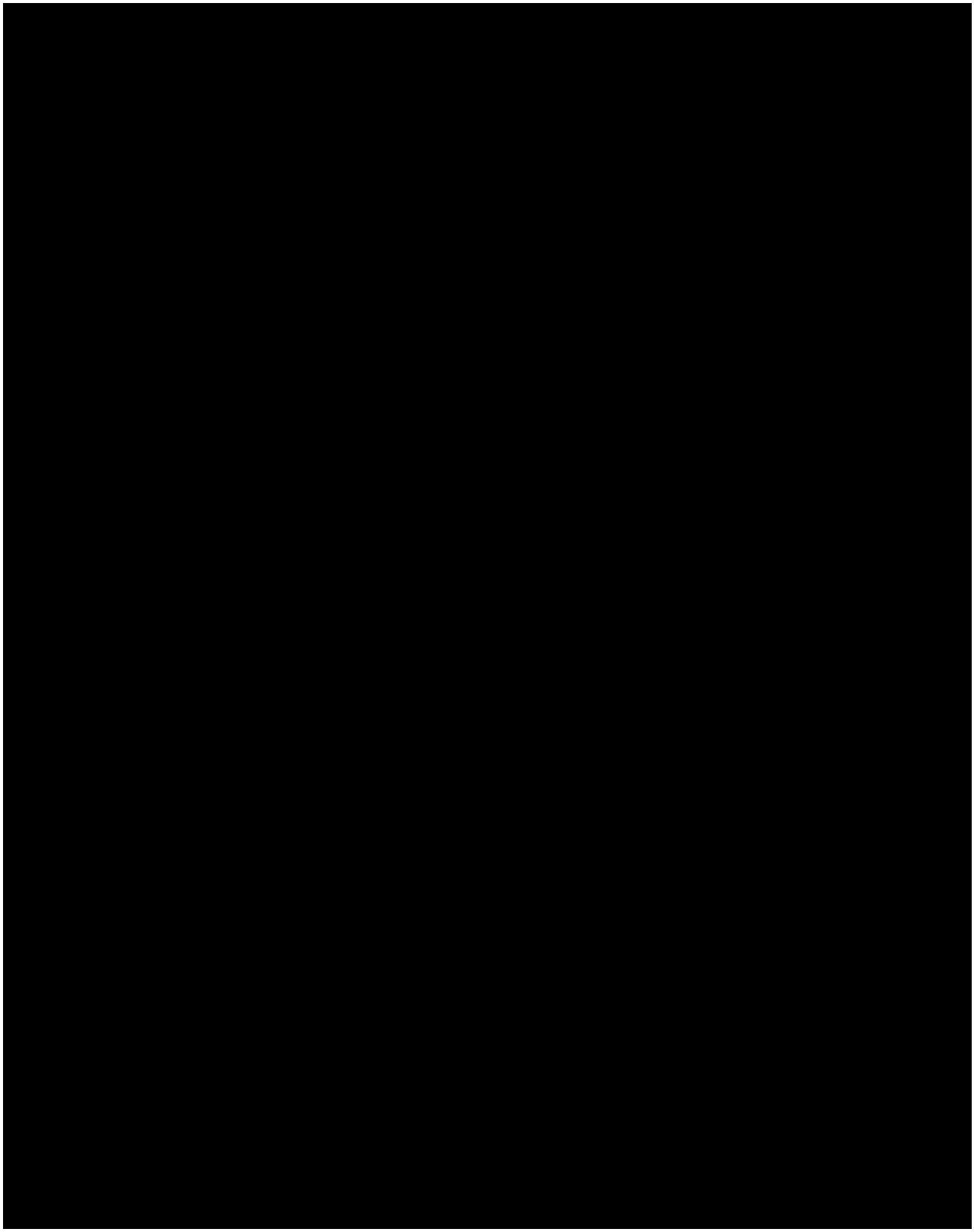
*Commercial in Confidence* *1*







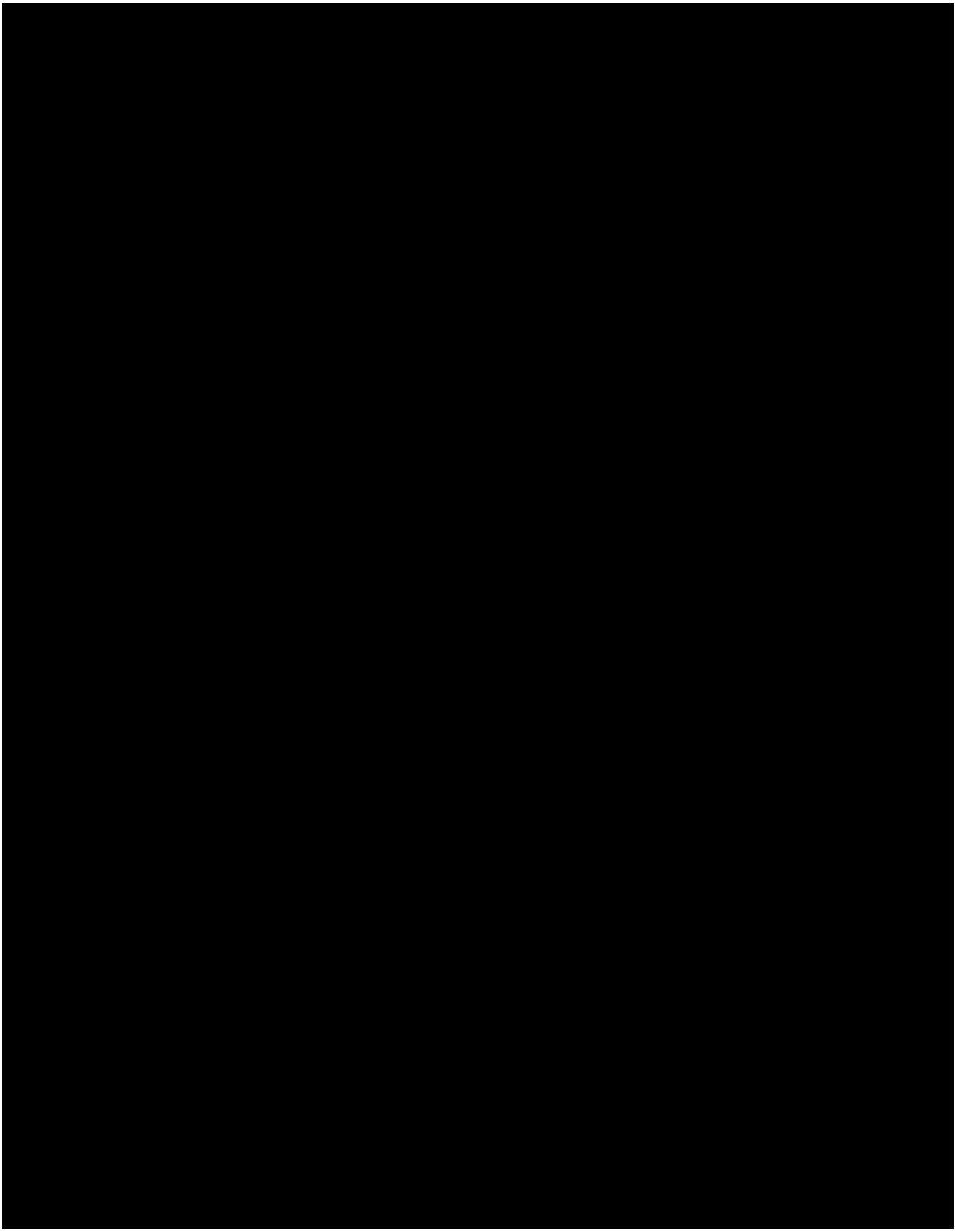
*Commercial in Confidence* *4*



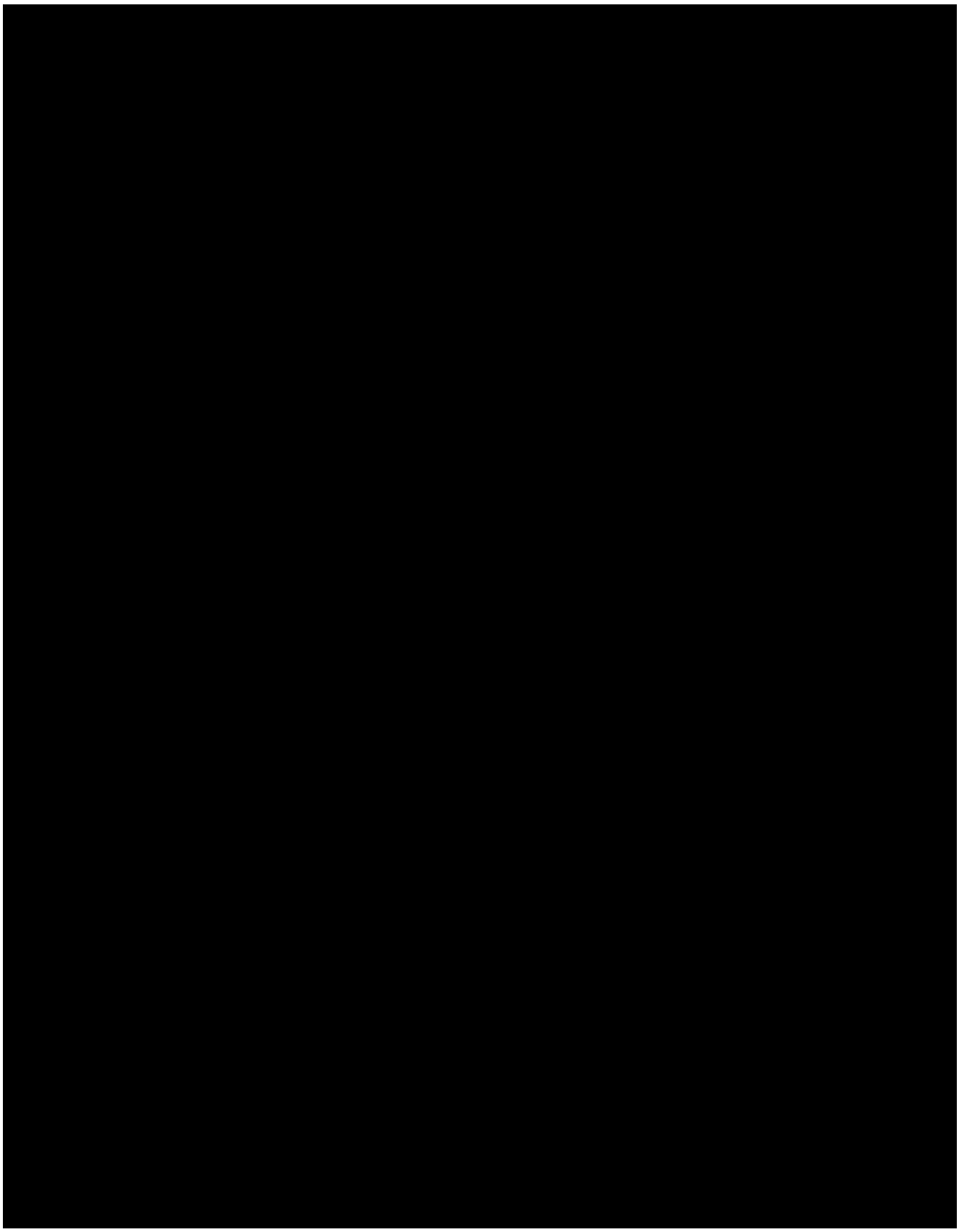

**Question: Describe the commitment your organisation will make to ensure that opportunities under the contract deliver the Policy Outcome and Award Criteria for MAC 2.2 - Create employment and training opportunities particularly for those who face barriers to employment and/or who are located in deprived areas, and for people in industries with known skills shortages or in high growth sectors.**

**How will you contribute to creating valuable employment and training opportunities through the delivery of this contract to help accelerate action for growth, jobs, contemporary skills and equity to thrive and adapt in a fast-changing environment? Please also detail how you will monitor the social value benefits delivered over the long-term.**

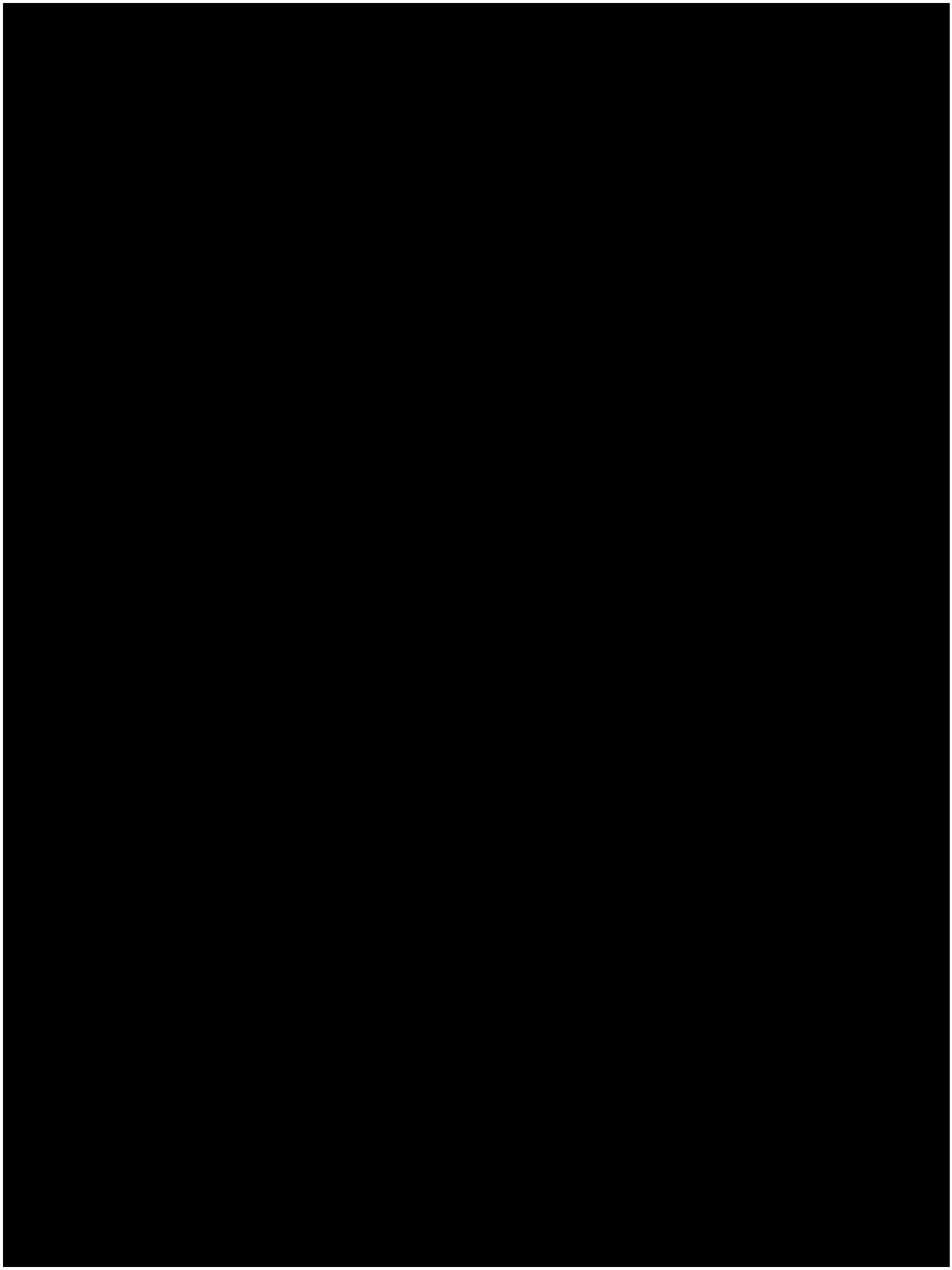
*Commercial in Confidence* *1*



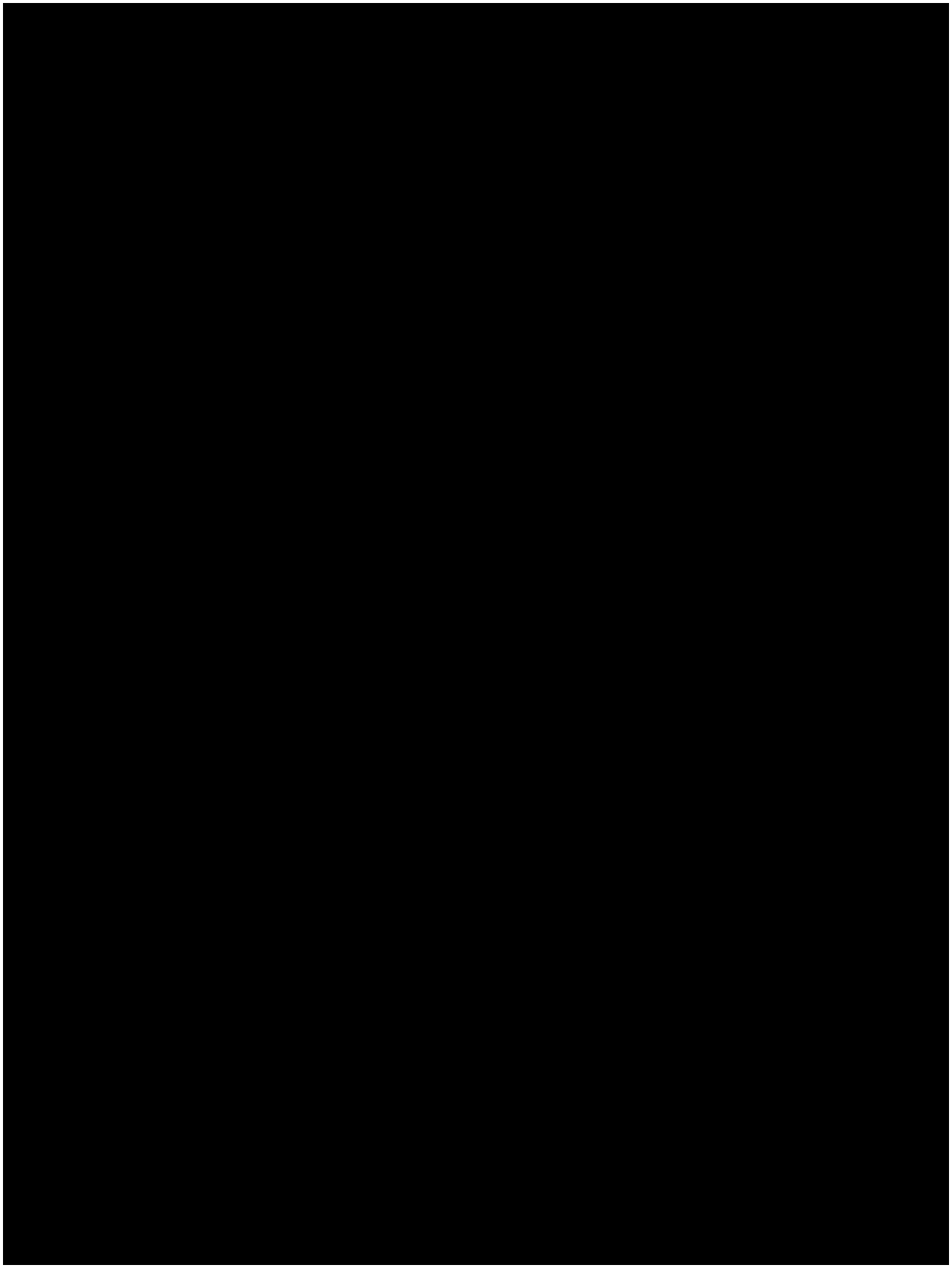
*Commercial in Confidence* *2*

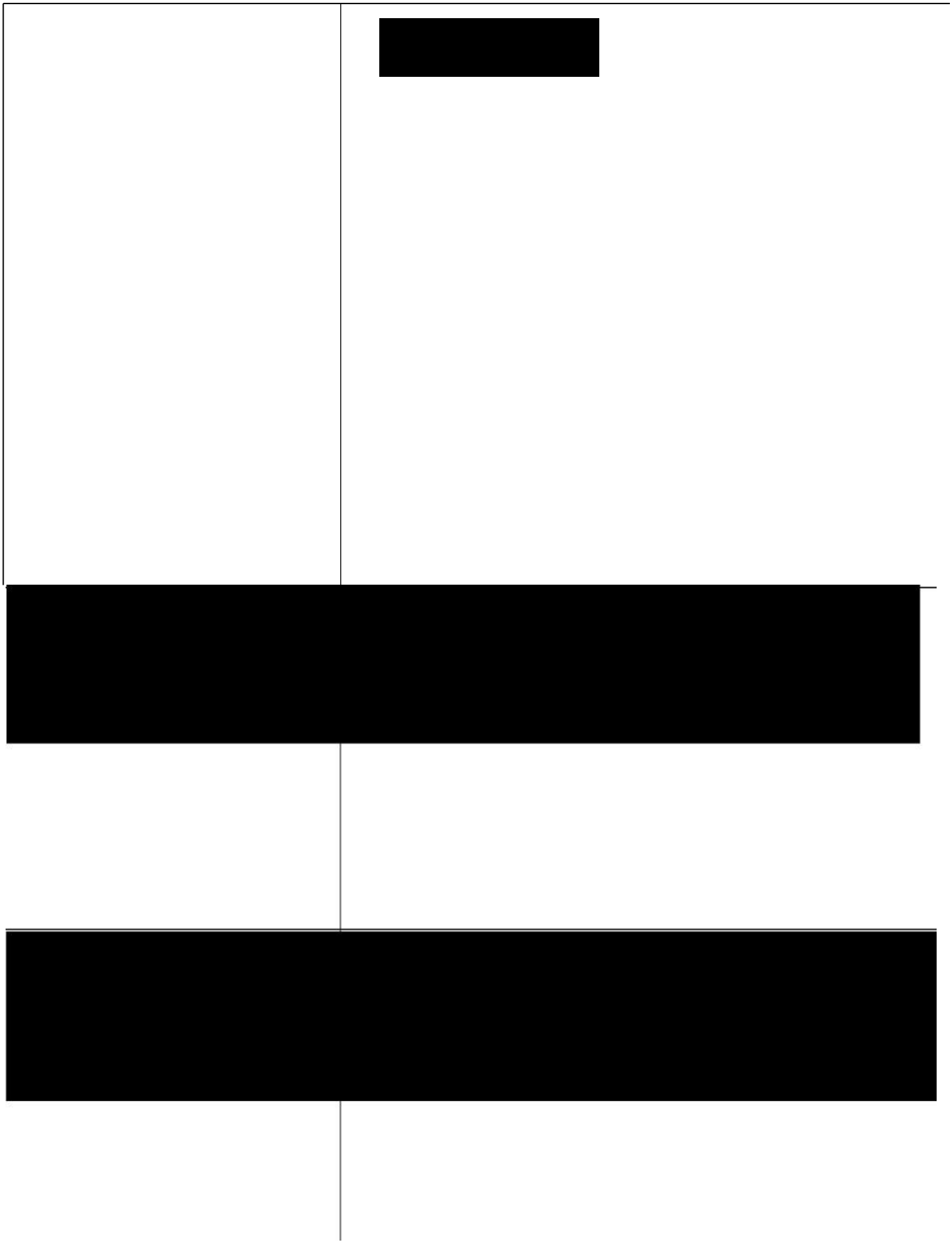


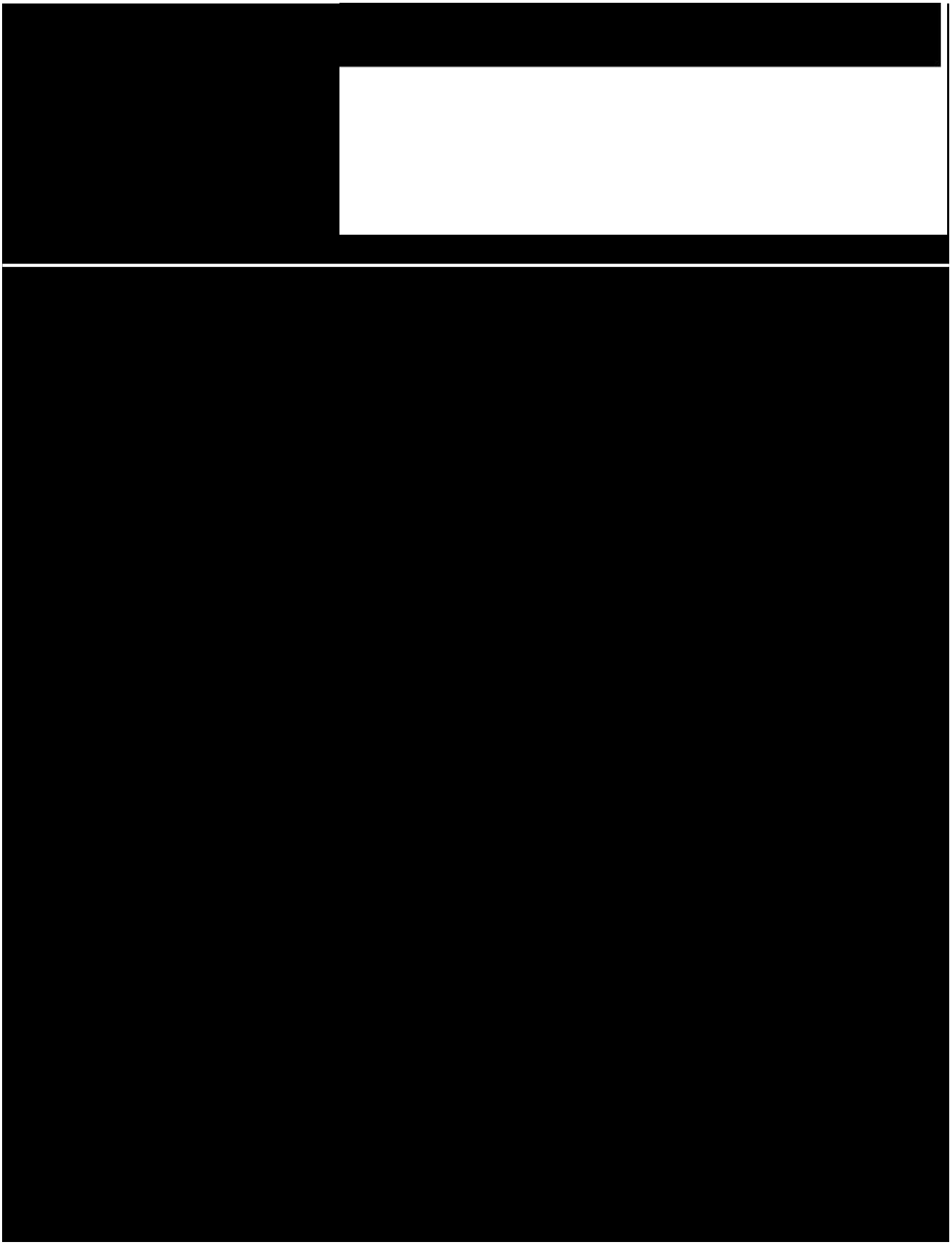
*Commercial in Confidence* *3*

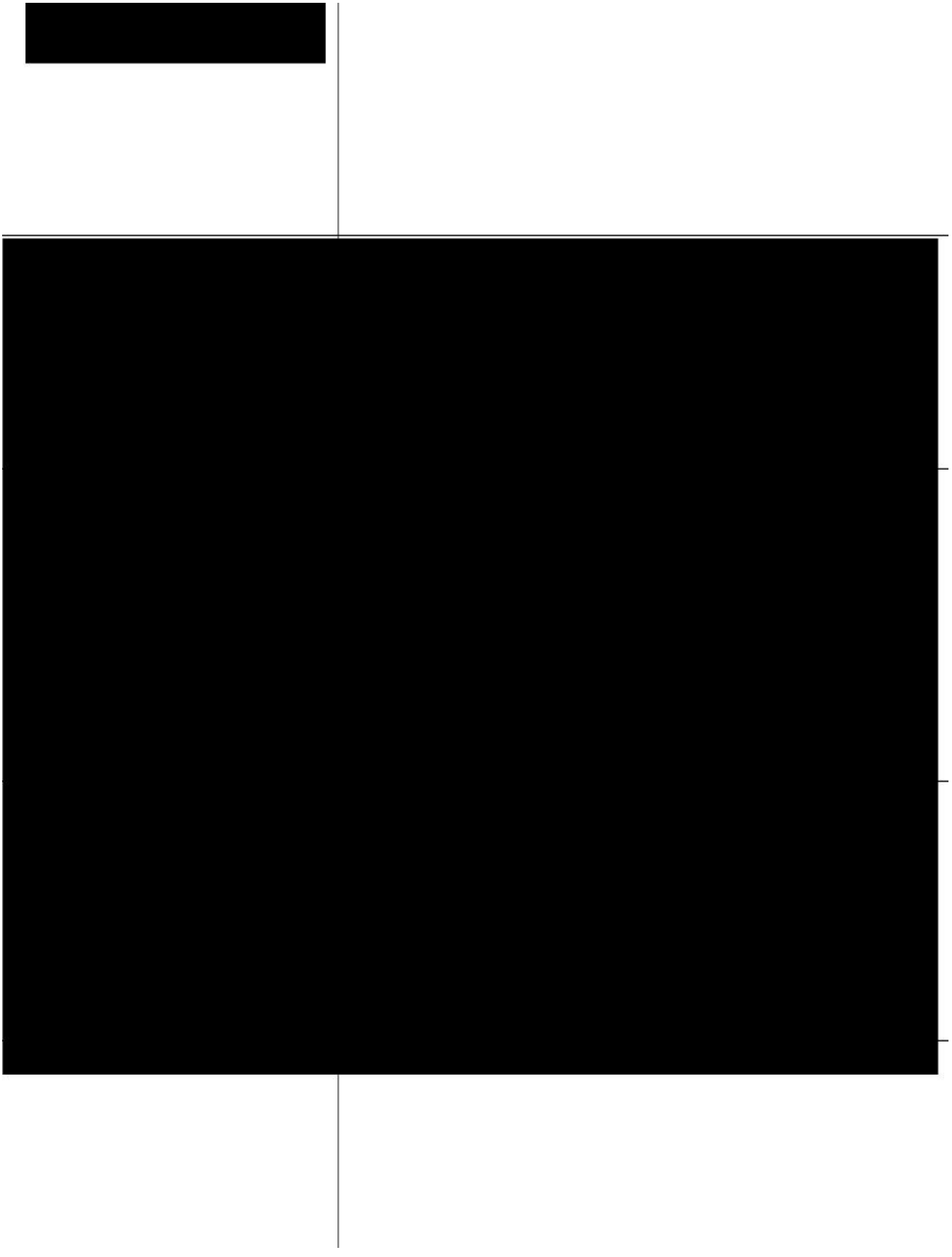


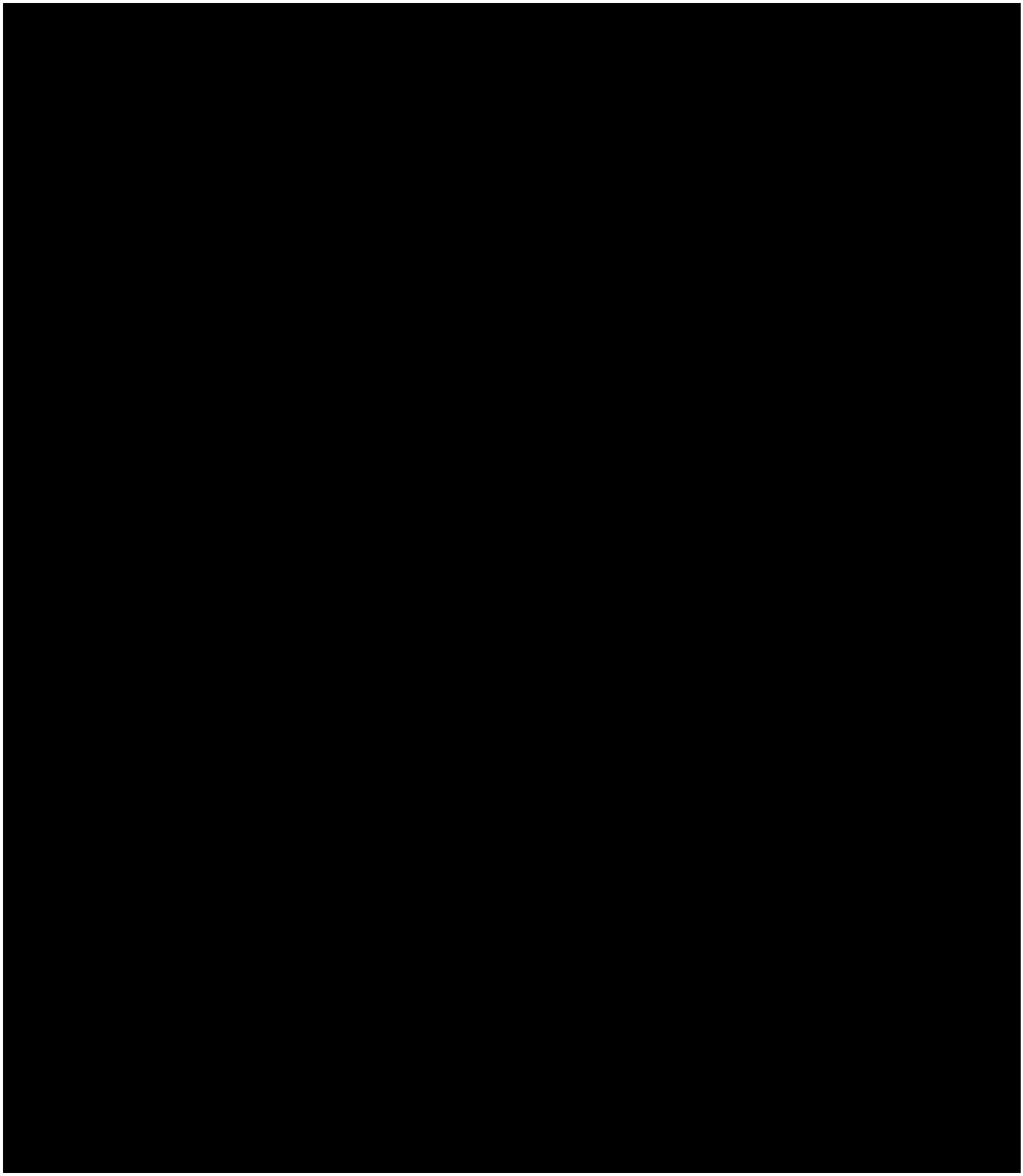
*Commercial in Confidence* *4*

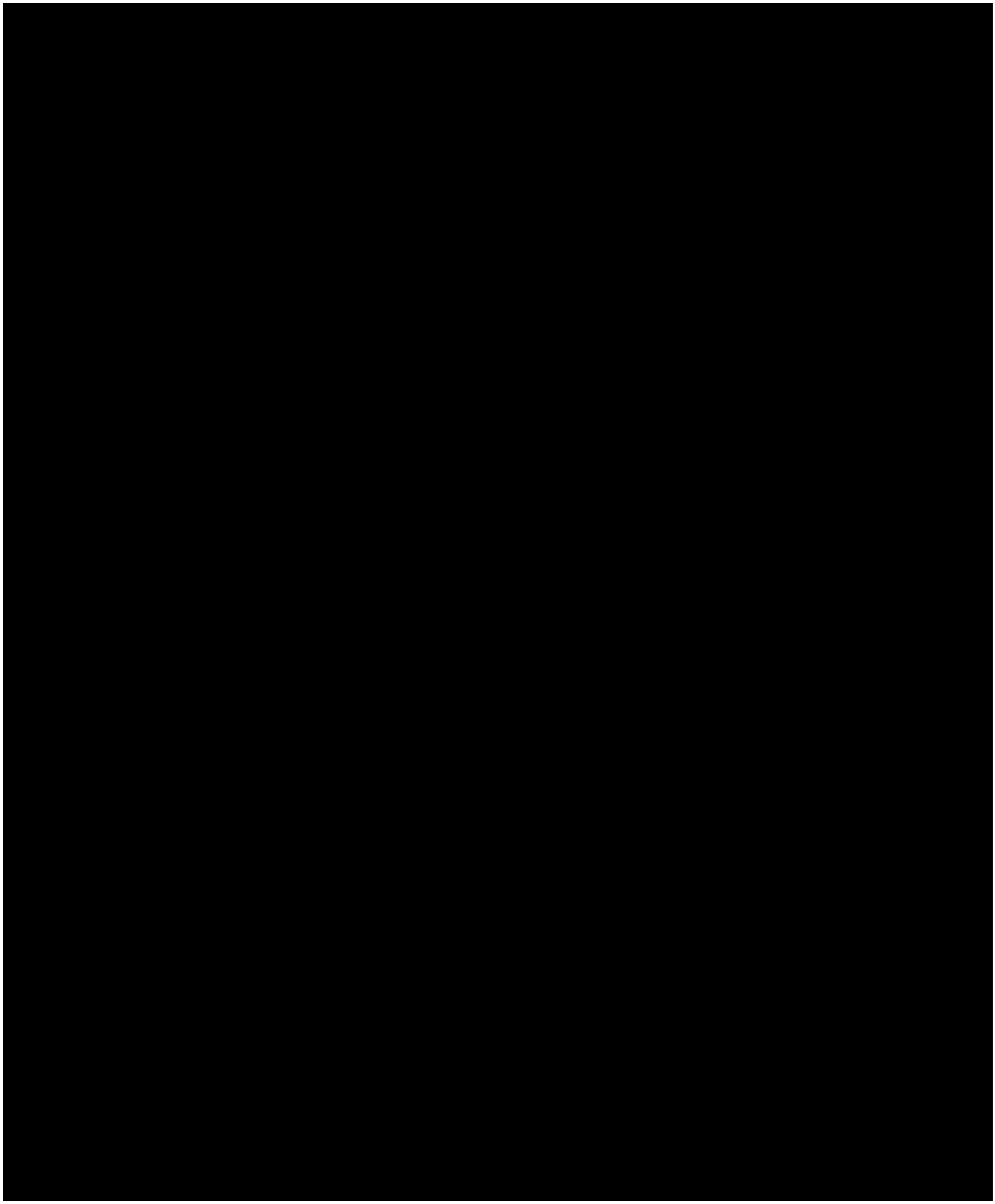


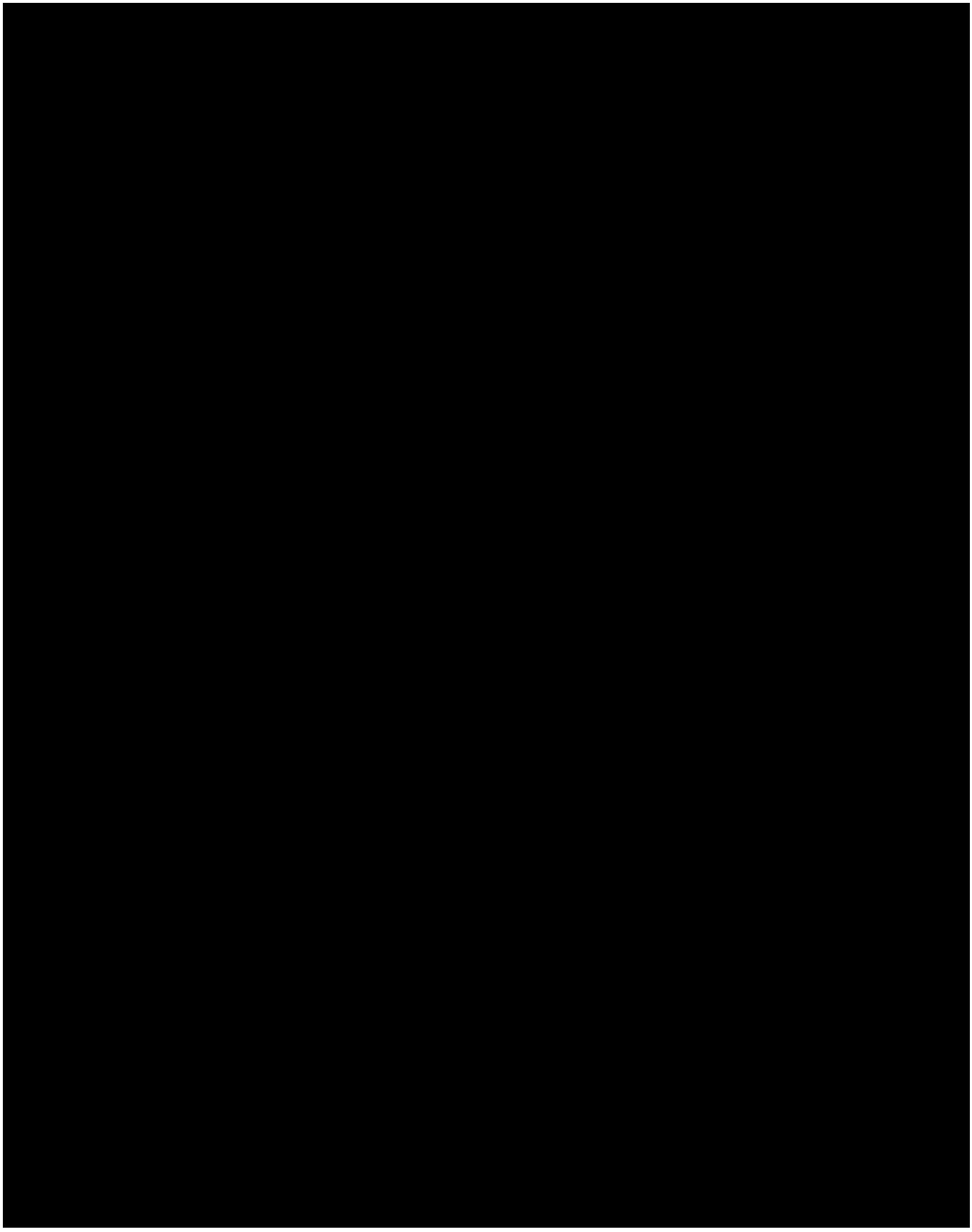


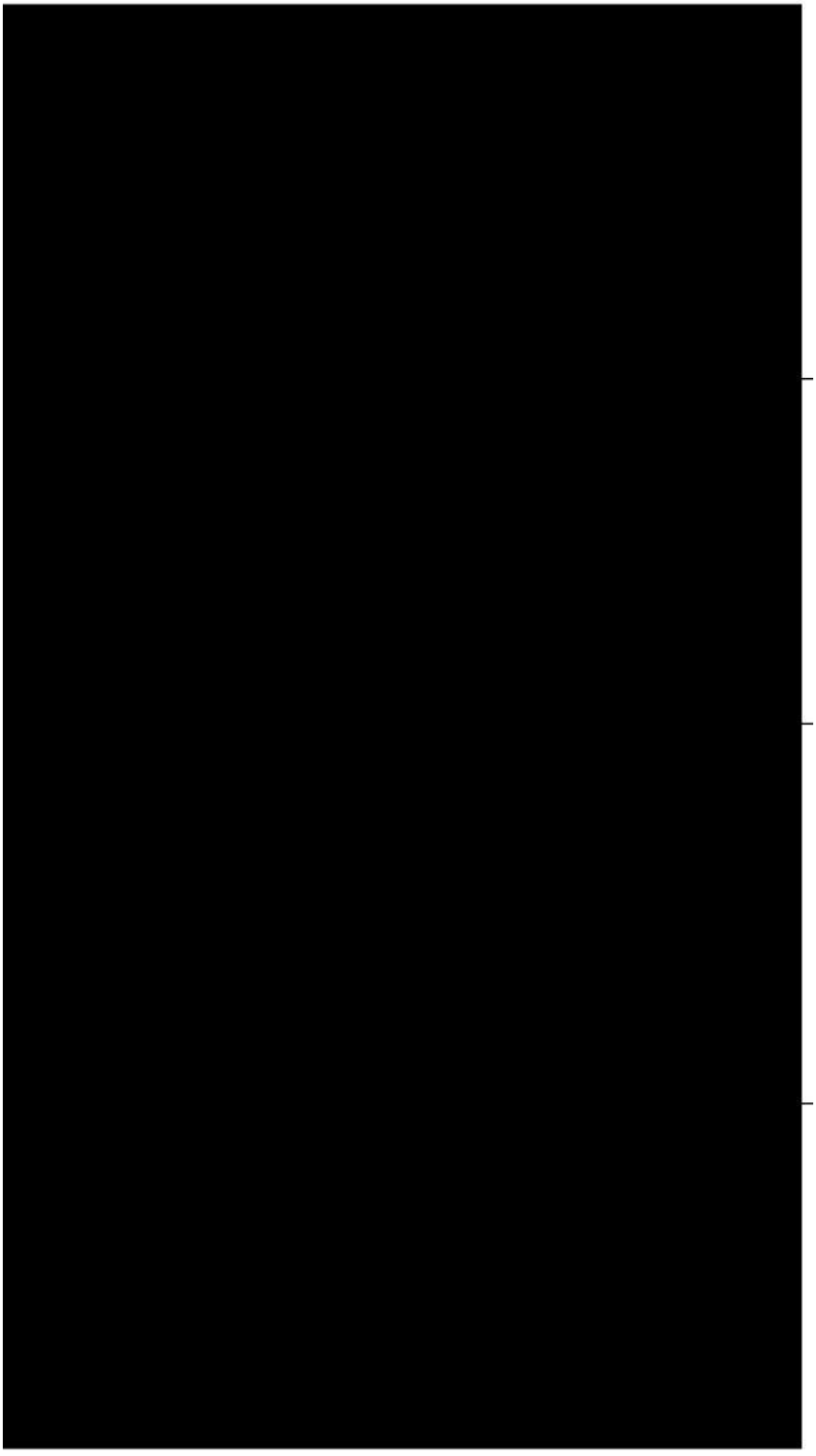


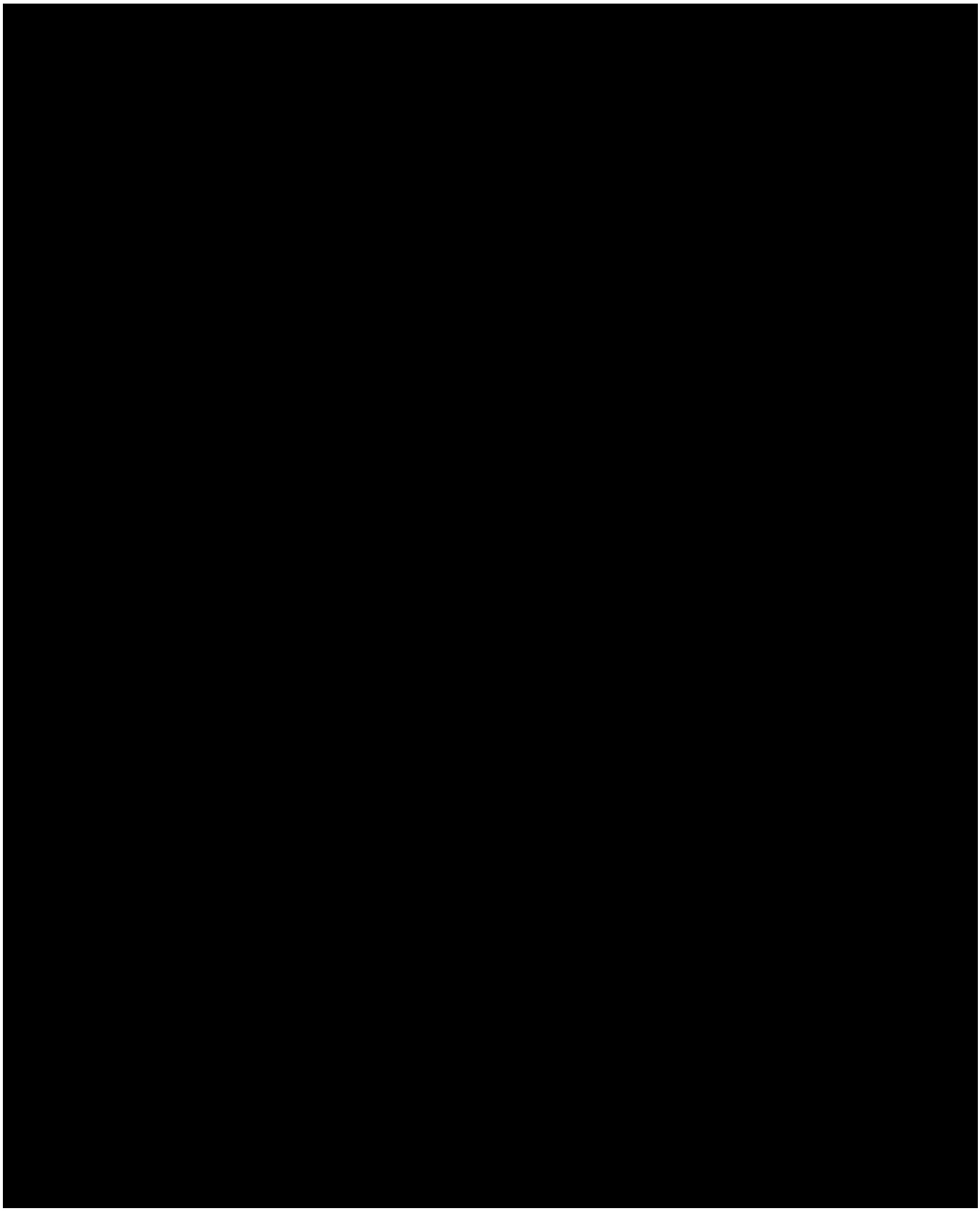


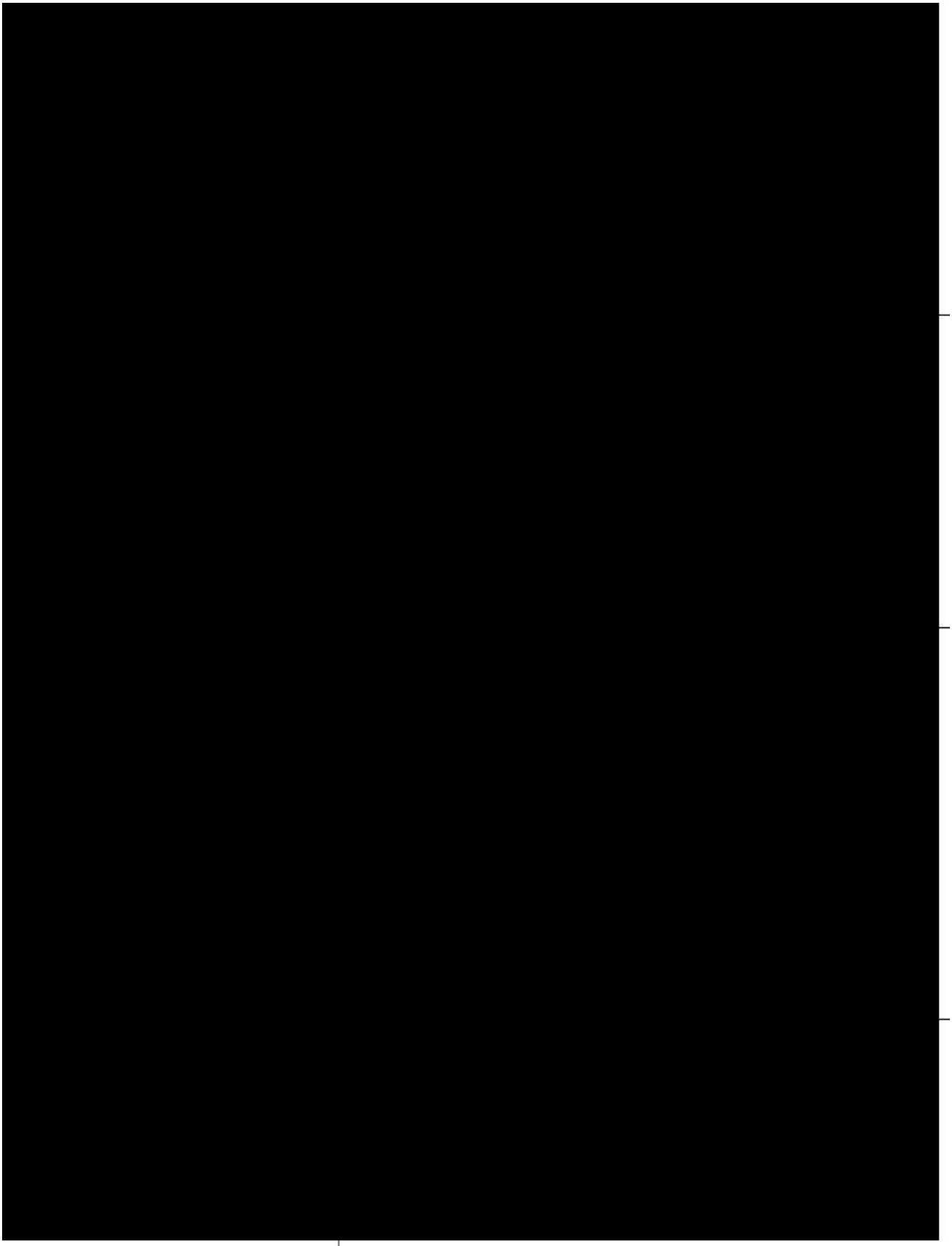


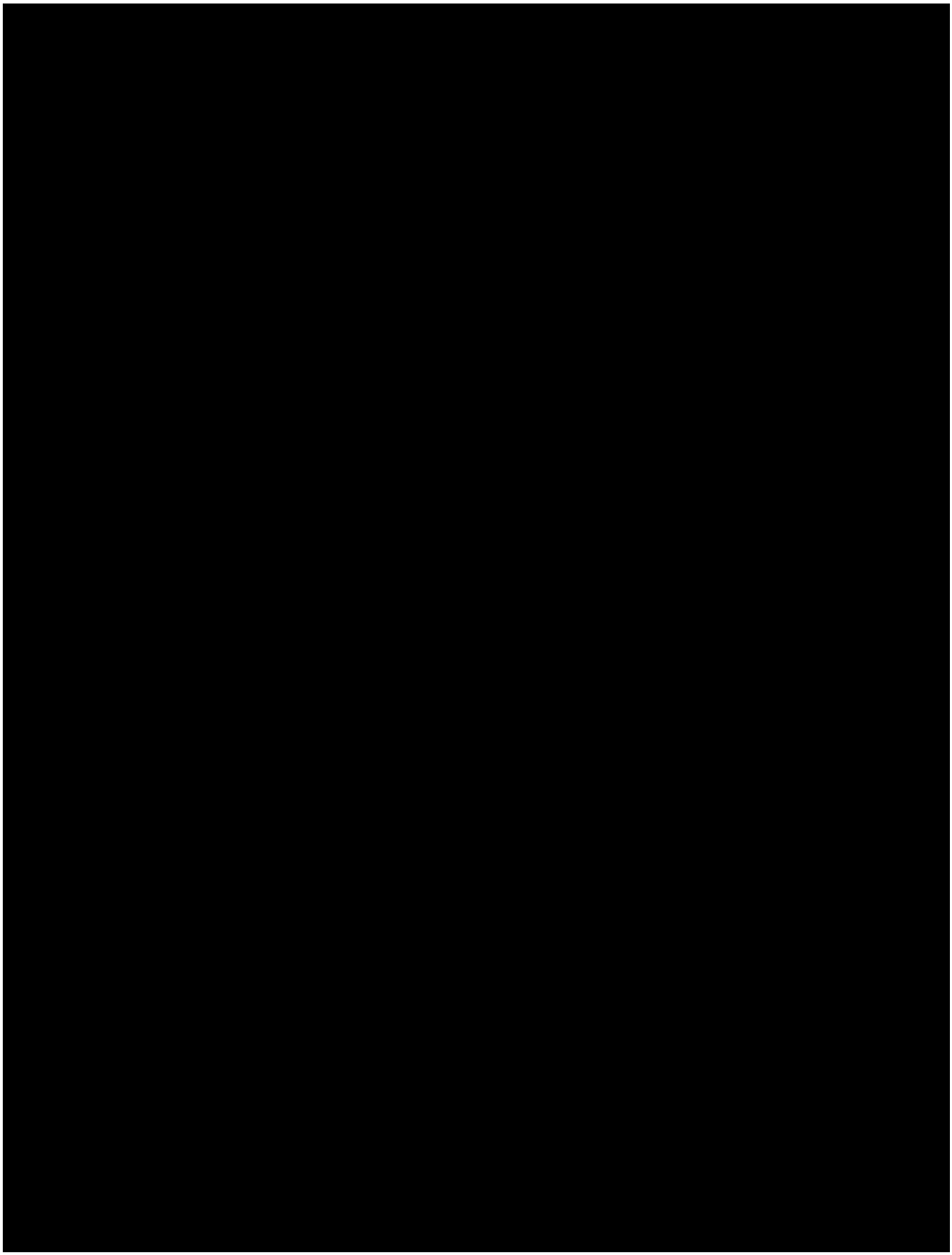










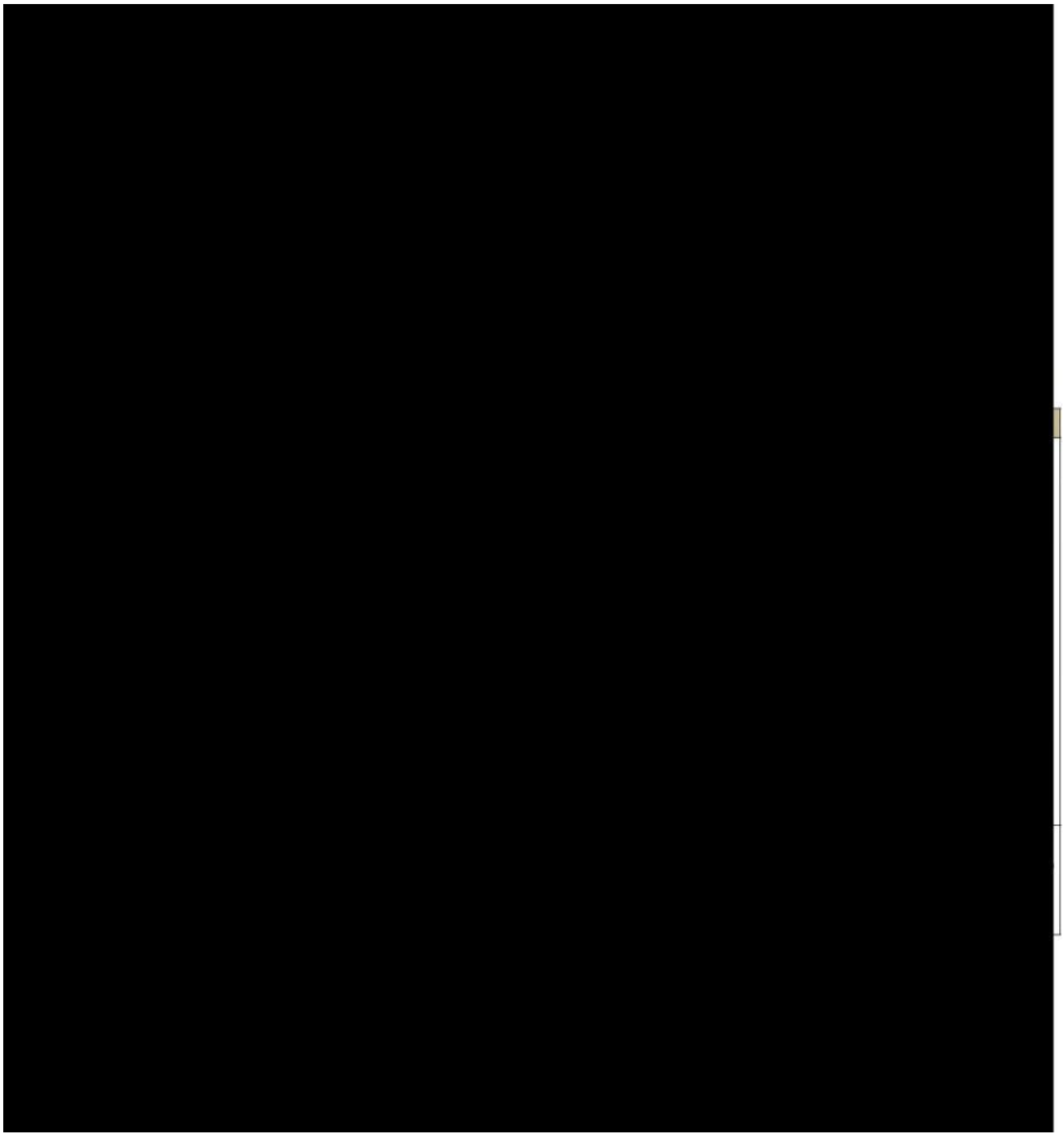


[redacted]

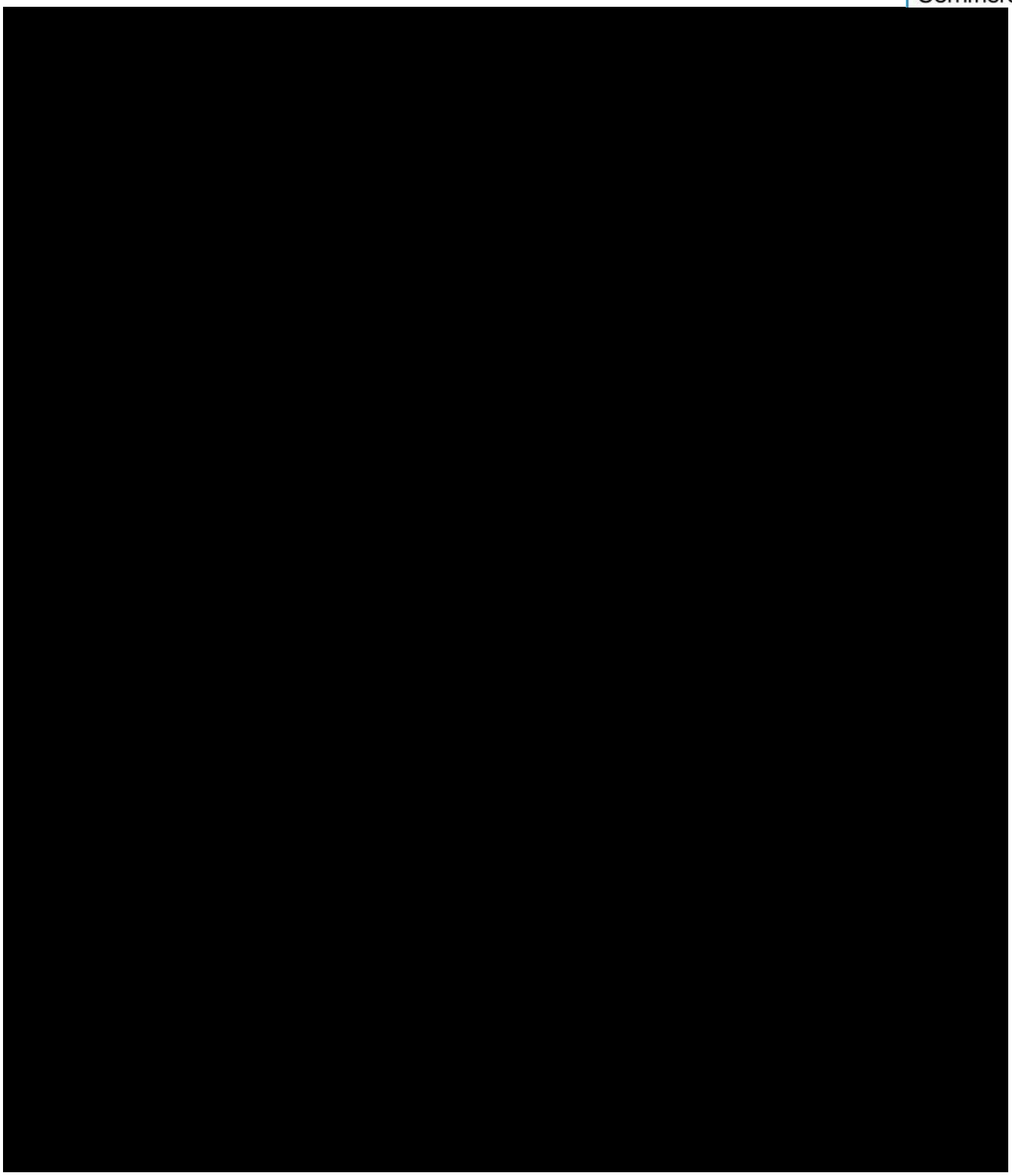


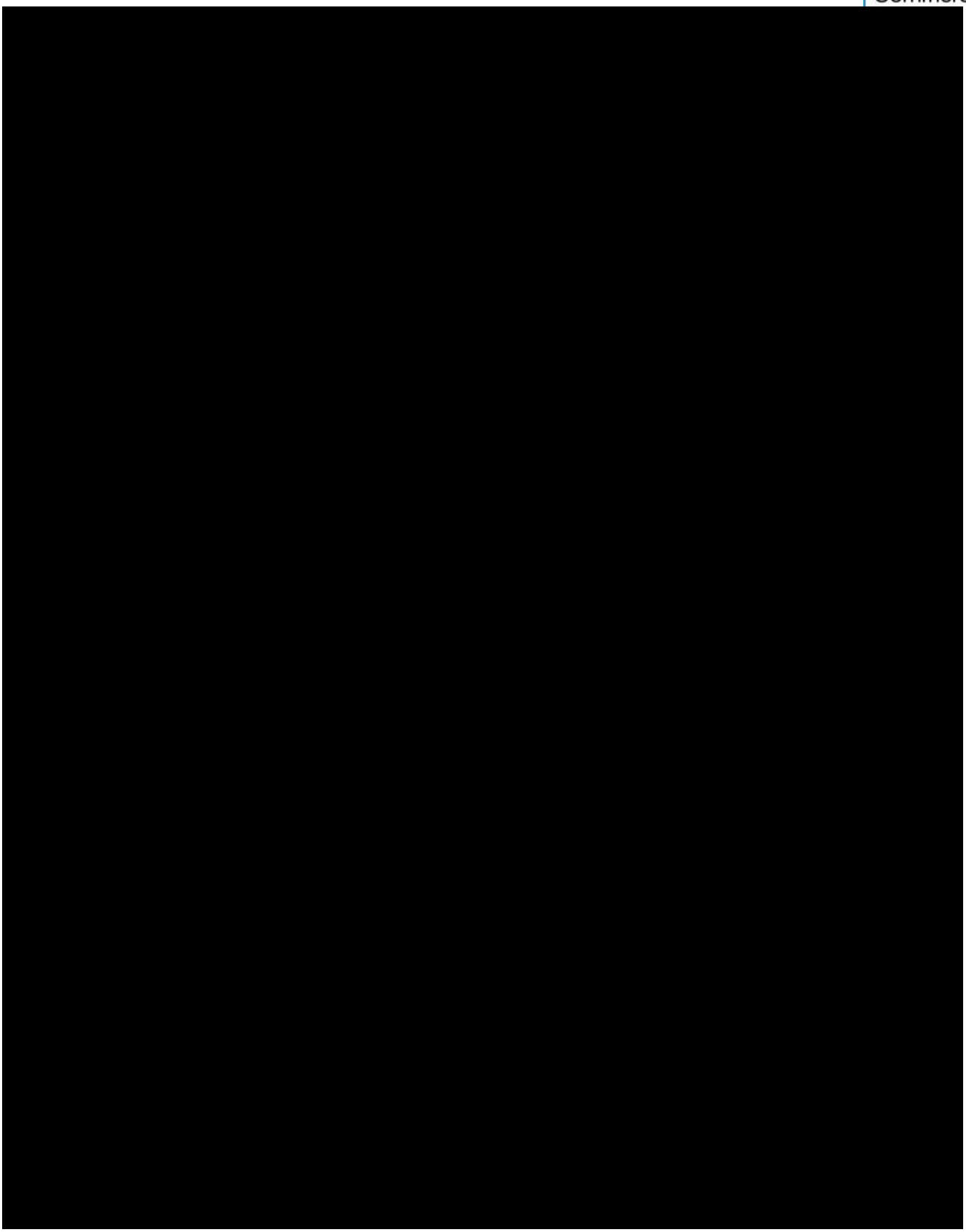

Crown Commercial Service

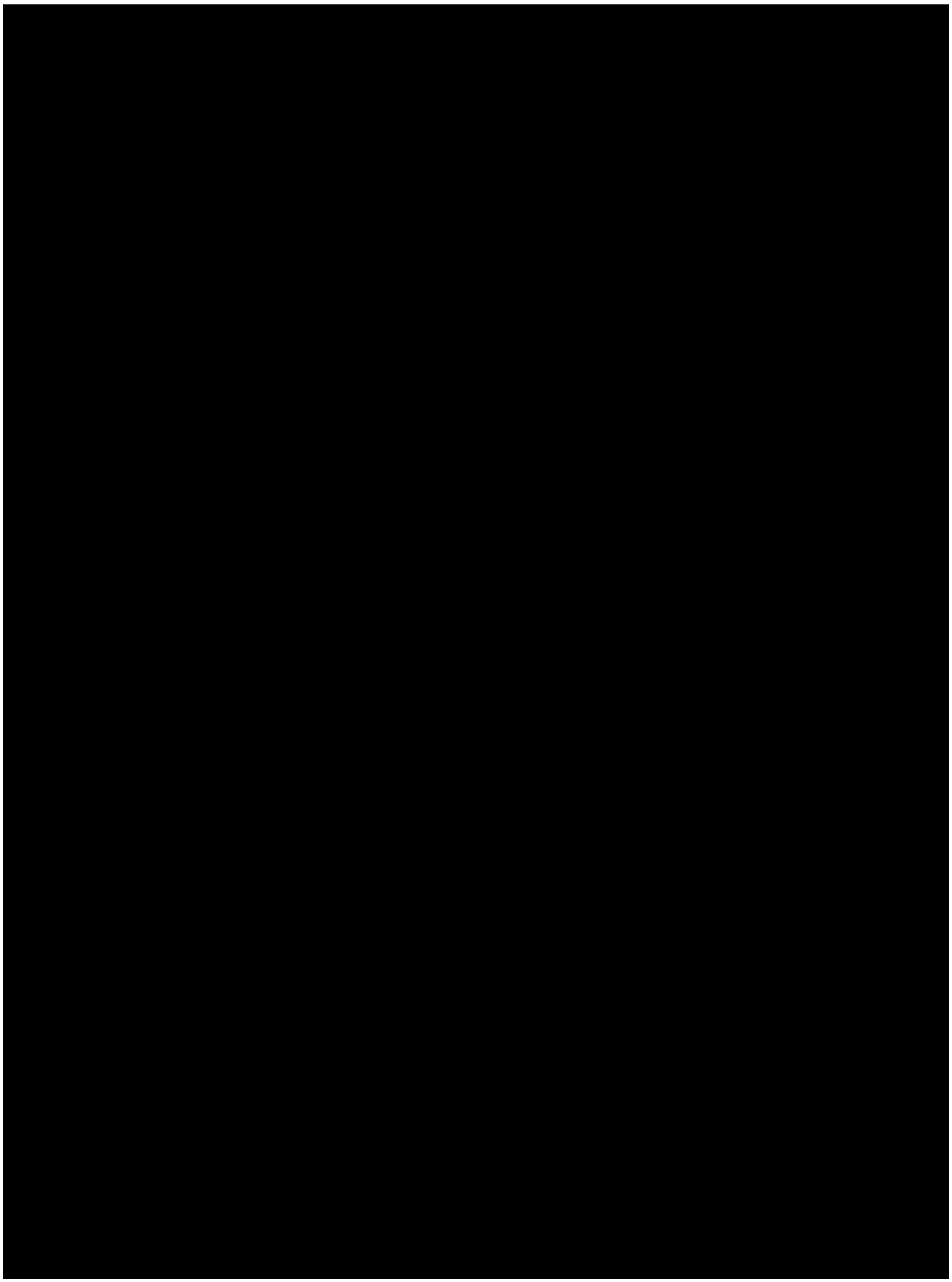
# Call-Off Schedule 5 (Pricing Details)



Ref: RM3830
FM Project Version: 1.A







# Call-Off Schedule 6 (ICT Services)

## 1. Definitions

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

| | |
|---|---|
| 5.4 **"Buyer Property"** | 5.5 the property, other than real property and IPR, including the Buyer System, any equipment issued or made available to the Supplier by the Buyer in connection with this Contract; |
| 5.6 **"Buyer Software"** | 5.7 any software which is owned by or licensed to the Buyer and which is or will be used by the Supplier for the purposes of providing the Deliverables; |
| 5.8 **"Buyer System"** | 5.9 the Buyer's computing environment (consisting of hardware, software and/or telecommunications networks or equipment) used by the Buyer or the Supplier in connection with this Contract which is owned by or licensed to the Buyer by a third party and which interfaces with the Supplier System or which is necessary for the Buyer to receive the Deliverables; |
| 5.10 **"Commercial off the shelf Software" or "COTS Software"** | 5.11 Non-customised software where the IPR may be owned and licensed either by the Supplier or a third party depending on the context, and which is commercially available for purchase and subject to standard licence terms |
| 5.12 **"Defect"** | any of the following:<br>any error, damage or defect in the manufacturing of a Deliverable; or<br>any error or failure of code within the Software which causes a Deliverable to malfunction or to produce unintelligible or incorrect results; or<br>any failure of any Deliverable to provide the performance, features and functionality specified in the requirements of the Buyer or the Documentation (including any adverse effect on response times) |
| 5.13 | |

| | |
|---|---|
| | regardless of whether or not it prevents the relevant Deliverable from passing any Test required under this Call Off Contract; or<br>any failure of any Deliverable to operate in conjunction with or interface with any other Deliverable in order to provide the performance, features and functionality specified in the requirements of the Buyer or the Documentation (including any adverse effect on response times) regardless of whether or not it prevents the relevant Deliverable from passing any Test required under this Contract; |
| 5.14 **"Emergency Maintenance"** | 5.15 ad hoc and unplanned maintenance provided by the Supplier where either Party reasonably suspects that the ICT Environment or the Services, or any part of the ICT Environment or the Services, has or may have developed a fault; |
| 5.16 **"ICT Environment"** | 5.17 the Buyer System and the Supplier System; |
| 5.18 **"Licensed Software"** | 5.19 all and any Software licensed by or through the Supplier, its Sub-Contractors or any third party to the Buyer for the purposes of or pursuant to this Call Off Contract, including any COTS Software; |
| 5.20 **"Maintenance Schedule"** | 5.21 has the meaning given to it in paragraph 8 of this Schedule; |
| 5.22 **"Malicious Software"** | 5.23 any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on program files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed, and whether the malicious software is introduced wilfully, negligently or without knowledge of its existence; |
| | 5.25 an item produced primarily to extend, alter or improve the Software and/or any Deliverable by providing additional functionality or performance enhancement |

| | |
|---|---|
| | (whether or not defects in the Software and/or Deliverable are also corrected) while still retaining the original designated purpose of that item; |
| 5.26 **"Open Source Software"** | 5.27 computer software that has its source code made available subject to an open-source licence under which the owner of the copyright and other IPR in such software provides the rights to use, study, change and distribute the software to any and all persons and for any and all purposes free of charge; |
| 5.28 **"Operating Environment"** | 5.29 means the Buyer System and any premises (including the Buyer Premises, the Supplier's premises or third party premises) from, to or at which:<br>the Deliverables are (or are to be) provided; or<br>the Supplier manages, organises or otherwise directs the provision or the use of the Deliverables; or<br>where any part of the Supplier System is situated; |
| 5.30 **"Permitted Maintenance"** | 5.31 has the meaning given to it in paragraph 8.2 of this Schedule; |
| 5.32 **"Quality** | 5.33 has the meaning given to it in paragraph 6.1 of this Schedule; |
| 5.34 **"Sites"** | 5.35 has the meaning given to it in Joint Schedule 1(Definitions), and for the purposes of this Call Off Schedule shall also include any premises from, to or at which physical interface with the Buyer System takes place; |
| 5.36 **"Software"** | 5.37 Specially Written Software COTS Software and non-COTS Supplier and third party Software; |
| 5.38 **"Software Supporting Materials"** | 5.39 has the meaning given to it in paragraph 9.1 of this Schedule; |
| 5.40 **"Source Code"** | 5.41 computer programs and/or data in eye-readable form and in such form that it can be compiled or interpreted into equivalent binary code together with all related design |

| | |
|---|---|
| | comments, flow charts, technical information and documentation necessary for the use, reproduction, maintenance, modification and enhancement of such software; |
| 5.42 **"Specially Written Software"** | 5.43 any software (including database software, linking instructions, test scripts, compilation instructions and test instructions) created by the Supplier (or by a Sub-Contractor or other third party on behalf of the Supplier) specifically for the purposes of this Contract, including any modifications or enhancements to COTS Software. For the avoidance of doubt Specially Written Software does not constitute New IPR; |
| 5.44 | 5.45 |
| 5.46 **"Supplier System"** | 5.47 the information and communications technology system used by the Supplier in supplying the Deliverables, including the COTS Software, the Supplier Equipment, configuration and management utilities, calibration and testing tools and related cabling (but excluding the Buyer |
| 5.48 | 5.49 |

## 2. When this Schedule should be used

2.1. This Schedule is designed to provide additional provisions necessary to facilitate the provision of ICT Services which are part of the Deliverables.

## 3. Buyer due diligence requirements

3.1. The Supplier shall satisfy itself of all relevant details, including but not limited to, details relating to the following;

3.1.1. suitability of the existing and (to the extent that it is defined or reasonably foreseeable at the Start Date) future Operating Environment;

3.1.2. operating processes and procedures and the working methods of the Buyer;

3.1.3. ownership, functionality, capacity, condition and suitability for use in the provision of the Deliverables of the Buyer Assets; and

3.1.4. existing contracts (including any licences, support, maintenance and other contracts relating to the Operating Environment) referred to in

the Due Diligence Information which may be novated to, assigned to or managed by the Supplier under this Contract and/or which the Supplier will require the benefit of for the provision of the Deliverables.

3.2. The Supplier confirms that it has advised the Buyer in writing of:

3.2.1. each aspect, if any, of the Operating Environment that is not suitable for the provision of the ICT Services;

3.2.2. the actions needed to remedy each such unsuitable aspect; and

3.2.3. a timetable for and the costs of those actions.

## 0. Licensed software warranty

4.1. The Supplier represents and warrants that:

4.1.1. it has and shall continue to have all necessary rights in and to the Licensed Software made available by the Supplier (and/or any Sub-Contractor) to the Buyer which are necessary for the performance of the Supplier's obligations under this Contract including the receipt of the Deliverables by the Buyer;

4.1.2. all components of the Specially Written Software shall:

4.1.2.1. be free from material design and programming errors;

4.1.2.2. perform in all material respects in accordance with the relevant specifications contained in Call Off Schedule 14 (Service Levels) and Documentation; and

4.1.2.3. not infringe any IPR.

## 1. Provision of ICT Services

5.1. The Supplier shall:

5.1.1. ensure that the release of any new COTS Software in which the Supplier owns the IPR, or upgrade to any Software in which the Supplier owns the IPR complies with the interface requirements of the Buyer and (except in relation to new Software or upgrades which are released to address Malicious Software) shall notify the Buyer three (3) Months before the release of any new COTS Software or Upgrade;

5.1.2. ensure that all Software including upgrades, updates and New Releases used by or on behalf of the Supplier are currently supported versions of that Software and perform in all material respects in accordance with the relevant specification;

5.1.3. ensure that the Supplier System will be free of all encumbrances;

5.1.4. ensure that the Deliverables are fully compatible with any Buyer Software, Buyer System, or otherwise used by the Supplier in connection with this Contract;

5.1.5. minimise any disruption to the Services and the ICT Environment and/or the Buyer's operations when providing the Deliverables;

## 4. Standards and Quality Requirements

6.1. The Supplier shall develop, in the timescales specified in the Order Form, quality plans that ensure that all aspects of the Deliverables are the subject of quality management systems and are consistent with BS EN ISO 9001 or any equivalent standard which is generally recognised as having replaced it ("**Quality Plans**")**.**

6.2. The Supplier shall seek Approval from the Buyer (not be unreasonably withheld or delayed) of the Quality Plans before implementing them. Approval shall not act as an endorsement of the Quality Plans and shall not relieve the Supplier of its responsibility for ensuring that the Deliverables are provided to the standard required by this Contract.

6.3. Following the approval of the Quality Plans, the Supplier shall provide all Deliverables in accordance with the Quality Plans.

6.4. The Supplier shall ensure that the Supplier Personnel shall at all times during the Call Off Contract Period:

6.4.1. be appropriately experienced, qualified and trained to supply the Deliverables in accordance with this Contract;

6.4.2. apply all due skill, care, diligence in faithfully performing those duties and exercising such powers as necessary in connection with the provision of the Deliverables; and

6.4.3. obey all lawful instructions and reasonable directions of the Buyer (including, if so required by the Buyer, the ICT Policy) and provide the Deliverables to the reasonable satisfaction of the Buyer.

## 5. ICT Audit

7.1. The Supplier shall allow any auditor access to the Supplier premises to:

7.1.1. inspect the ICT Environment and the wider service delivery environment (or any part of them);

7.1.2. review any records created during the design and development of the Supplier System and pre-operational environment such as information relating to Testing;

7.1.3. review the Supplier’s quality management systems including all relevant Quality Plans.

## 2. Maintenance of the ICT Environment

8.1. If specified by the Buyer in the Order Form, the Supplier shall create and maintain a rolling schedule of planned maintenance to the ICT Environment ("**Maintenance Schedule**") and make it available to the Buyer for Approval in accordance with the timetable and instructions specified by the Buyer.

8.2. Once the Maintenance Schedule has been Approved, the Supplier shall only undertake such planned maintenance (which shall be known as "**Permitted Maintenance**") in accordance with the Maintenance Schedule.

8.3. The Supplier shall give as much notice as is reasonably practicable to the Buyer prior to carrying out any Emergency Maintenance.

8.4. The Supplier shall carry out any necessary maintenance (whether Permitted Maintenance or Emergency Maintenance) where it reasonably suspects that the ICT Environment and/or the Services or any part thereof has or may have developed a fault. Any such maintenance shall be carried out in such a manner and at such times so as to avoid (or where this is not possible so as to minimise) disruption to the ICT Environment and the provision of the Deliverables.

## 3. Intellectual Property Rights in ICT

9.1. **Assignments granted by the Supplier: Specially Written Software**

9.1.1. The Supplier assigns (by present assignment of future rights to take effect immediately on it coming into existence) to the Buyer with full guarantee (or shall procure assignment to the Buyer), title to and all rights and interest in the Specially Written Software together with and including:

9.1.1.1. the Documentation, Source Code and the Object Code of the Specially Written Software; and

9.1.1.2. all build instructions, test instructions, test scripts, test data, operating instructions and other documents and tools necessary for maintaining and supporting the Specially Written Software and the New IPR (together the "**Software Supporting Materials**").

9.1.2. The Supplier shall:

9.1.2.1. inform the Buyer of all Specially Written Software or New IPRs that are a modification, customisation, configuration or enhancement to any COTS Software;

9.1.2.2. deliver to the Buyer the Specially Written Software and any computer program elements of the New IPRs in both Source Code and Object Code forms together with relevant Documentation and all related Software Supporting Materials within seven days of completion or, if a relevant Milestone has been identified in an Implementation Plan,

Achievement of that Milestone and shall provide updates of them promptly following each new release of the Specially Written Software, in each case on media that is reasonably acceptable to the Buyer and the Buyer shall become the owner of such media upon receipt; and

9.1.2.3. without prejudice to paragraph 9.1.2.2, provide full details to the Buyer of any of the Supplier's Existing IPRs or Third Party IPRs which are embedded or which are an integral part of the Specially Written Software or New IPR and the Supplier hereby grants to the Buyer and shall procure that any relevant third party licensor shall grant to the Buyer a perpetual, irrevocable, non-exclusive, assignable, royalty-free licence to use, sub-license and/or commercially exploit such Supplier's Existing IPRs and Third Party IPRs to the extent that it is necessary to enable the Buyer to obtain the full benefits of ownership of the Specially Written Software and New IPRs.

9.1.3. The Supplier shall promptly execute all such assignments as are required to ensure that any rights in the Specially Written Software and New IPRs are properly transferred to the Buyer.

9.2. **Licences for non-COTS IPR from the Supplier and third parties to the Buyer**

9.2.1. Unless the Buyer gives its Approval the Supplier must not use any:

a) of its own Existing IPR that is not COTS Software;

b) third party software that is not COTS Software

9.2.2. Where the Buyer Approves the use of the Supplier's Existing IPR that is not COTS Software the Supplier shall grants to the Buyer a perpetual, royalty-free and non-exclusive licence to use adapt, and sub-license the same for any purpose relating to the Deliverables (or substantially equivalent deliverables) or for any purpose relating to the exercise of the Buyer's (or, if the Buyer is a Central Government Body, any other Central Government Body's) business or function including the right to load, execute, store, transmit, display and copy (for the purposes of archiving, backing-up, loading, execution, storage, transmission or display) for the Call Off Contract Period and after expiry of the Contract to the extent necessary to ensure continuity of service and an effective transition of Services to a Replacement Supplier.

9.2.3. Where the Buyer Approves the use of third party Software that is not COTS Software the Supplier shall procure that the owners or the authorised licensors of any such Software grant a direct licence to the Buyer on terms at least equivalent to those set out in Paragraph 9.2.2. If the Supplier cannot obtain such a licence for the Buyer it shall:

9.2.3.1. notify the Buyer in writing giving details of what licence terms can be obtained and whether there are alternative software providers which the Supplier could seek to use; and

9.2.3.2. only use such third party IPR as referred to at paragraph 9.2.3.1 if the Buyer Approves the terms of the licence from the relevant third party.

9.2.4. Where the Supplier is unable to provide a license to the Supplier's Existing IPR in accordance with Paragraph 9.2.2 above, it must meet the requirement by making use of COTS Software or Specially Written Software.

9.2.5. The Supplier may terminate a licence granted under paragraph 9.2.1 by giving at least thirty (30) days' notice in writing if there is an Authority Cause which constitutes a material Default which, if capable of remedy, is not remedied within twenty (20) Working Days after the Supplier gives the Buyer written notice specifying the breach and requiring its remedy.

9.3. **Licenses for COTS Software by the Supplier and third parties to the Buyer**

9.3.1. The Supplier shall either grant, or procure that the owners or the authorised licensors of any COTS Software grant, a direct licence to the Buyer on terms no less favourable than those standard commercial terms on which such software is usually made commercially available.

9.3.2. Where the Supplier owns the COTS Software it shall make available the COTS software to a Replacement Supplier at a price and on terms no less favourable than those standard commercial terms on which such software is usually made commercially available.

9.3.3. Where a third party is the owner of COTS Software licensed in accordance with this Paragraph 9.3 the Supplier shall support the Replacement Supplier to make arrangements with the owner or authorised licencee to renew the license at a price and on terms no less favourable than those standard commercial terms on which such software is usually made commercially available.

9.3.4. The Supplier shall notify the Buyer within seven (7) days of becoming aware of any COTS Software which in the next thirty-six (36) months:

9.3.4.1. will no longer be maintained or supported by the developer; or

9.3.4.2. will no longer be made commercially available

9.4. **Buyer's right to assign/novate licences**

9.4.1. The Buyer may assign, novate or otherwise transfer its rights and obligations under the licences granted pursuant to paragraph 9.2 (to:

9.4.1.1. a Central Government Body; or

9.4.1.2. to any body (including any private sector body) which performs or carries on any of the functions and/or activities that previously had been performed and/or carried on by the Buyer.

9.4.2. If the Buyer ceases to be a Central Government Body, the successor body to the Buyer shall still be entitled to the benefit of the licences granted in paragraph 9.2.

9.5. **Licence granted by the Buyer**

9.5.1. The Buyer grants to the Supplier a royalty-free, non-exclusive, non-transferable licence during the Contract Period to use the Buyer Software and the Specially Written Software solely to the extent necessary for providing the Deliverables in accordance with this Contract, including the right to grant sub-licences to Sub-Contractors provided that any relevant Sub-Contractor has entered into a confidentiality undertaking with the Supplier on the same terms as set out in Clause 15 (Confidentiality).

9.6. **Open Source Publication**

9.6.1. Unless the Buyer otherwise agrees in advance in writing (and subject to paragraph 9.6.3) all Specially Written Software and computer program elements of New IPR shall be created in a format, or able to be converted (in which case the Supplier shall also provide the converted format to the Buyer) into a format, which is:

9.6.1.1. suitable for publication by the Buyer as Open Source; and

9.6.1.2. based on Open Standards (where applicable),

5.49.1 and the Buyer may, at its sole discretion, publish the same as Open Source.

9.6.2. The Supplier hereby warrants that the Specially Written Software and the New IPR:

9.6.2.1. are suitable for release as Open Source and that the Supplier has used reasonable endeavours when developing the same to ensure that publication by the Buyer will not enable a third party to use them in any way which could reasonably be foreseen to compromise the operation, running or security of the Specially Written Software, New IPRs or the Buyer System;

9.6.2.2. have been developed using reasonable endeavours to ensure that their publication by the Buyer shall not cause any harm or damage to any party using them;

9.6.2.3. do not contain any material which would bring the Buyer into disrepute;

9.6.2.4. can be published as Open Source without breaching the rights of any third party;

9.6.2.5. will be supplied in a format suitable for publication as Open Source ("**the Open Source Publication Material**") no later than the date notified by the Buyer to the Supplier; and

9.6.2.6. do not contain any Malicious Software.

9.6.3. Where the Buyer has Approved a request by the Supplier for any part of the Specially Written Software or New IPRs to be excluded from the requirement to be in an Open Source format due to the intention to embed or integrate Supplier Existing IPRs and/or Third Party IPRs (and where the Parties agree that such IPRs are not intended to be published as Open Source), the Supplier shall:

9.6.3.1. as soon as reasonably practicable, provide written details of the nature of the IPRs and items or Deliverables based on IPRs which are to be excluded from Open Source publication; and

9.6.3.2. include in the written details and information about the impact that inclusion of such IPRs or Deliverables based on such IPRs, will have on any other Specially Written Software and/or New IPRs and the Buyer's ability to publish such other items or Deliverables as Open Source.

9.7. **Malicious Software**

9.7.1. The Supplier shall, throughout the Contract Period, use the latest versions of anti-virus definitions and software available from an industry accepted anti-virus software vendor to check for, contain the spread of, and minimise the impact of Malicious Software.

9.7.2. If Malicious Software is found, the Parties shall co-operate to reduce the effect of the Malicious Software and, particularly if Malicious Software causes loss of operational efficiency or loss or corruption of Government Data, assist each other to mitigate any losses and to restore the provision of the Deliverables to its desired operating efficiency.

9.7.3. Any cost arising out of the actions of the Parties taken in compliance with the provisions of paragraph 9.7.2 shall be borne by the Parties as follows:

9.7.3.1. by the Supplier, where the Malicious Software originates from the Supplier Software, the third party Software supplied by the Supplier or the Government Data (whilst the Government Data was under the control of the Supplier) unless the Supplier can demonstrate that such Malicious

Software was present and not quarantined or otherwise identified by the Buyer when provided to the Supplier; and

9.7.3.2. by the Buyer, if the Malicious Software originates from the Buyer Software or the Buyer Data (whilst the Buyer Data was under the control of the Buyer).

# Call-Off Schedule 8 (Business Continuity and Disaster Recovery)

## 1. Definitions

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

| | |
|---|---|
| **"BCDR Plan"** | 1 has the meaning given to it in Paragraph 2.2 of this Schedule; |
| **"Business Continuity Plan"** | 2 has the meaning given to it in Paragraph 2.3.2 of this Schedule; |
| **"Disaster"** | 3 the occurrence of one or more events which, either separately or cumulatively, mean that the Deliverables, or a material part thereof will be unavailable (or could reasonably be anticipated to be unavailable); |
| **"Disaster Recovery Deliverables"** | 4 the Deliverables embodied in the processes and procedures for restoring the provision of Deliverables following the occurrence of a Disaster; |
| **"Disaster Recovery Plan"** | 5 has the meaning given to it in Paragraph 2.3.3 of this Schedule; |
| **"Disaster Recovery System"** | 6 the system embodied in the processes and procedures for restoring the provision of Deliverables following the occurrence of a Disaster; |
| **"Related Supplier"** | 7 any person who provides Deliverables to the Buyer which are related to the Deliverables from time to time; |
| **"Review Report"** | 8 has the meaning given to it in Paragraph 6.3 of this Schedule; and |
| **"Supplier's Proposals"** | 9 has the meaning given to it in Paragraph 6.3 of this Schedule; |

## 2. BCDR Plan

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

2.2 At least ninety (90) Working Days prior to the Start Date the Supplier shall prepare and deliver to the Buyer for the Buyer's written approval a plan (a **"BCDR Plan"**), which shall detail the processes and arrangements that the Supplier shall follow to:

2.2.1 ensure continuity of the business processes and operations supported by the Services following any failure or disruption of any element of the Deliverables; and

2.2.2 the recovery of the Deliverables in the event of a Disaster

2.3 The BCDR Plan shall be divided into three sections:

2.3.1 Section 1 which shall set out general principles applicable to the BCDR Plan;

2.3.2 Section 2 which shall relate to business continuity (the **"Business Continuity Plan"**); and

2.3.3 Section 3 which shall relate to disaster recovery (the **"Disaster Recovery Plan"**).

2.4 Following receipt of the draft BCDR Plan from the Supplier, the Parties shall use reasonable endeavours to agree the contents of the BCDR Plan. If the Parties are unable to agree the contents of the BCDR Plan within twenty (20) Working Days of its submission, then such Dispute shall be resolved in accordance with the Dispute Resolution Procedure.

## 3. General Principles of the BCDR Plan (Section 1)

3.1 Section 1 of the BCDR Plan shall:

3.1.1 set out how the business continuity and disaster recovery elements of the BCDR Plan link to each other;

3.1.2 provide details of how the invocation of any element of the BCDR Plan may impact upon the provision of the Deliverables and any goods and/or services provided to the Buyer by a Related Supplier;

3.1.3 contain an obligation upon the Supplier to liaise with the Buyer and any Related Suppliers with respect to business continuity and disaster recovery;

3.1.4 detail how the BCDR Plan interoperates with any overarching disaster recovery or business continuity plan of the Buyer and any of its other Related

Supplier in each case as notified to the Supplier by the Buyer from time to time;

3.1.5 contain a communication strategy including details of an incident and problem management service and advice and help desk facility which can be accessed via multiple channels;

3.1.6 contain a risk analysis, including:

(a) failure or disruption scenarios and assessments of likely frequency of occurrence;

(b) identification of any single points of failure within the provision of Deliverables and processes for managing those risks;

(c) identification of risks arising from the interaction of the provision of Deliverables with the goods and/or services provided by a Related Supplier; and

(d) a business impact analysis of different anticipated failures or disruptions;

3.1.7 provide for documentation of processes, including business processes, and procedures;

3.1.8 set out key contact details for the Supplier (and any Subcontractors) and for the Buyer;

3.1.9 identify the procedures for reverting to "normal service";

3.1.10 set out method(s) of recovering or updating data collected (or which ought to have been collected) during a failure or disruption to minimise data loss;

3.1.11 identify the responsibilities (if any) that the Buyer has agreed it will assume in the event of the invocation of the BCDR Plan; and

3.1.12 provide for the provision of technical assistance to key contacts at the Buyer as required by the Buyer to inform decisions in support of the Buyer's business continuity plans.

3.2 The BCDR Plan shall be designed so as to ensure that:

3.2.1 the Deliverables are provided in accordance with this Contract at all times during and after the invocation of the BCDR Plan;

3.2.2 the adverse impact of any Disaster is minimised as far as reasonably possible;

3.2.3 it complies with the relevant provisions of ISO/IEC 27002; ISO22301/ISO22313 and all other industry standards from time to time in force; and

3.2.4 it details a process for the management of disaster recovery testing.

3.3 The BCDR Plan shall be upgradeable and sufficiently flexible to support any changes to the Deliverables and the business operations supported by the provision of Deliverables.

3.4 The Supplier shall not be entitled to any relief from its obligations under the Performance Indicators (PI's) or Service levels, or to any increase in the Charges to the extent that a Disaster occurs as a consequence of any breach by the Supplier of this Contract.

## 4. Business Continuity (Section 2)

4.1 The Business Continuity Plan shall set out the arrangements that are to be invoked to ensure that the business processes facilitated by the provision of Deliverables remain supported and to ensure continuity of the business operations supported by the Services including:

4.1.1 the alternative processes, options and responsibilities that may be adopted in the event of a failure in or disruption to the provision of Deliverables; and

4.1.2 the steps to be taken by the Supplier upon resumption of the provision of Deliverables in order to address the effect of the failure or disruption.

4.2 The Business Continuity Plan shall:

4.2.1 address the various possible levels of failures of or disruptions to the provision of Deliverables;

4.2.2 set out the goods and/or services to be provided and the steps to be taken to remedy the different levels of failures of and disruption to the Deliverables;

4.2.3 specify any applicable Performance Indicators with respect to the provision of the Business Continuity Services and details of any agreed relaxation to the Performance Indicators (PI's) or Service Levels in respect of the provision of other Deliverables during any period of invocation of the Business Continuity Plan; and

4.2.4 set out the circumstances in which the Business Continuity Plan is invoked.

## 5. Disaster Recovery (Section 3)

5.1 The Disaster Recovery Plan (which shall be invoked only upon the occurrence of a Disaster) shall be designed to ensure that upon the occurrence of a Disaster the Supplier ensures continuity of the business operations of the Buyer supported by the Services following any Disaster or during any period of service failure or disruption with, as far as reasonably possible, minimal adverse impact.

5.2 The Supplier's BCDR Plan shall include an approach to business continuity and disaster recovery that addresses the following:

5.2.1 loss of access to the Buyer Premises;

5.2.2 loss of utilities to the Buyer Premises;

5.2.3 loss of the Supplier's helpdesk or CAFM system;

5.2.4 loss of a Subcontractor;

5.2.5 emergency notification and escalation process;

5.2.6 contact lists;

5.2.7 staff training and awareness;

5.2.8 BCDR Plan testing;

5.2.9 post implementation review process;

5.2.10 any applicable Performance Indicators (PI's) with respect to the provision of the disaster recovery services and details of any agreed relaxation to the Performance Indicators (PI's) or Service Levels in respect of the provision of other Deliverables during any period of invocation of the Disaster Recovery Plan;

5.2.11 details of how the Supplier shall ensure compliance with security standards ensuring that compliance is maintained for any period during which the Disaster Recovery Plan is invoked;

5.2.12 access controls to any disaster recovery sites used by the Supplier in relation to its obligations pursuant to this Schedule; and

5.2.13 testing and management arrangements.

## 6. Review and changing the BCDR Plan

6.1 The Supplier shall review the BCDR Plan:

6.1.1 on a regular basis and as a minimum once every six (6) Months;

6.1.2 within three (3) calendar Months of the BCDR Plan (or any part) having been invoked pursuant to Paragraph 7; and

6.1.3 where the Buyer requests in writing any additional reviews (over and above those provided for in Paragraphs 6.1.1 and 6.1.2 of this Schedule) whereupon the Supplier shall conduct such reviews in accordance with the Buyer's written requirements. Prior to starting its review, the Supplier shall provide an accurate written estimate of the total costs payable by the Buyer for the Buyer's approval. The costs of both Parties of any such additional reviews shall be met by the Buyer except that the Supplier shall not be entitled to charge the Buyer for any costs that it may incur above any estimate without the Buyer's prior written approval.

6.2 Each review of the BCDR Plan pursuant to Paragraph 6.1 shall assess its suitability having regard to any change to the Deliverables or any underlying business processes and operations facilitated by or supported by the Services which have taken place since the later of the original approval of the BCDR Plan or the last review of the BCDR Plan, and shall also have regard to any occurrence of any event since that date (or the likelihood of any such event taking place in the foreseeable

future) which may increase the likelihood of the need to invoke the BCDR Plan. The review shall be completed by the Supplier within such period as the Buyer shall reasonably require.

6.3 The Supplier shall, within twenty (20) Working Days of the conclusion of each such review of the BCDR Plan, provide to the Buyer a report (a **"Review Report"**) setting out the Supplier's proposals (the **"Supplier's Proposals"**) for addressing any changes in the risk profile and its proposals for amendments to the BCDR Plan.

6.4 Following receipt of the Review Report and the Supplier's Proposals, the Parties shall use reasonable endeavours to agree the Review Report and the Supplier's Proposals. If the Parties are unable to agree Review Report and the Supplier's Proposals within twenty (20) Working Days of its submission, then such Dispute shall be resolved in accordance with the Dispute Resolution Procedure.

6.5 The Supplier shall as soon as is reasonably practicable after receiving the approval of the Supplier's Proposals effect any change in its practices or procedures necessary so as to give effect to the Supplier's Proposals. Any such change shall be at the Supplier's expense unless it can be reasonably shown that the changes are required because of a material change to the risk profile of the Deliverables.

## 7. Testing the BCDR Plan

7.1 The Supplier shall test the BCDR Plan:

7.1.1 regularly and in any event not less than once in every Contract Year;

7.1.2 in the event of any major reconfiguration of the Deliverables

7.1.3 at any time where the Buyer considers it necessary (acting in its sole discretion).

7.2 If the Buyer requires an additional test of the BCDR Plan, it shall give the Supplier written notice and the Supplier shall conduct the test in accordance with the Buyer's requirements and the relevant provisions of the BCDR Plan. The Supplier's costs of the additional test shall be borne by the Buyer unless the BCDR Plan fails the additional test in which case the Supplier's costs of that failed test shall be borne by the Supplier.

7.3 The Supplier shall undertake and manage testing of the BCDR Plan in full consultation with and under the supervision of the Buyer and shall liaise with the Buyer in respect of the planning, performance, and review, of each test, and shall comply with the reasonable requirements of the Buyer.

7.4 The Supplier shall ensure that any use by it or any Subcontractor of "live" data in such testing is first approved with the Buyer. Copies of live test data used in any such testing shall be (if so required by the Buyer) destroyed or returned to the Buyer on completion of the test.

7.5 The Supplier shall, within twenty (20) Working Days of the conclusion of each test, provide to the Buyer a report setting out:

7.5.1 the outcome of the test;

7.5.2 any failures in the BCDR Plan (including the BCDR Plan's procedures) revealed by the test; and

7.5.3 the Supplier's proposals for remedying any such failures.

7.6 Following each test, the Supplier shall take all measures requested by the Buyer to remedy any failures in the BCDR Plan and such remedial activity and re-testing shall be completed by the Supplier, at its own cost, by the date reasonably required by the Buyer.

## 8. Invoking the BCDR Plan

8.1 In the event of a complete loss of service or in the event of a Disaster, the Supplier shall immediately invoke the BCDR Plan (and shall inform the Buyer promptly of such invocation). In all other instances the Supplier shall invoke or test the BCDR Plan only with the prior consent of the Buyer.

## 9. Circumstances beyond your control

9.1 The Supplier shall not be entitled to relief under Clause 20 (Circumstances beyond your control) if it would not have been impacted by the Force Majeure Event had it not failed to comply with its obligations under this Schedule.

# Call-Off Schedule 9 (Security)

## Part B: Long Form Security Requirements

### Definitions

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

**"Breach of Security"** 1 means the occurrence of:

a) any unauthorised access to or use of the Goods and/or Deliverables, the Sites and/or any Information and Communication Technology ("ICT"), information or data (including the Confidential Information and the Government Data) used by the Buyer and/or the Supplier in connection with this Contract; and/or

b) the loss and/or unauthorised disclosure of any information or data (including the Confidential Information and the Government Data), including any copies of such information or data, used by the Buyer and/or the Supplier in connection with this Contract,

2 in either case as more particularly set out in the security requirements in the Security Policy where the Buyer has required compliance therewith in accordance with paragraph 3.4.3 d;

**"ISMS"** 3 the information security management system and process developed by the Supplier in accordance with Paragraph 3 (ISMS) as updated from time to time in accordance with this Schedule; and

**"Security Tests"** 4 tests to validate the ISMS and security of all relevant processes, systems, incident response plans, patches to vulnerabilities and mitigations to Breaches of Security.

## Security Requirements

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

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

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

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

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

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

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

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

## Information Security Management System (ISMS)

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

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

The Buyer acknowledges that;

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

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

The ISMS shall:

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

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

at all times provide a level of security which:

is in accordance with the Law and this Contract;

complies with the Baseline Security Requirements;

as a minimum demonstrates Good Industry Practice;

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

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

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

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

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

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

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

document the security incident management processes and incident response plans;

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

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

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

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

If the bespoke ISMS submitted to the Buyer pursuant to Paragraph 3.3.1 is Approved by the Buyer, it shall be adopted by the Supplier immediately and thereafter operated and maintained in accordance with this Schedule. If the ISMS is not Approved by the Buyer, the Supplier shall amend it within ten (10) Working Days of a notice of non-approval from the Buyer and re-submit it to the Buyer for Approval. The Parties shall use all reasonable endeavours to ensure that the Approval process takes as little time as possible and in any event no longer than fifteen (15) Working Days from the date of the first submission of the ISMS to the Buyer. If the Buyer does not Approve the ISMS following its resubmission, the matter shall be resolved in accordance with the Dispute Resolution Procedure. No Approval to be given by the Buyer pursuant to this Paragraph 3 may be unreasonably withheld or delayed. However any failure to approve the ISMS on the grounds that it does not comply with any of the requirements set out in Paragraphs 3.4 to 3.6 shall be deemed to be reasonable.

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

## Security Management Plan

Within twenty (20) Working Days after the Start Date, the Supplier shall prepare and submit to the Buyer for Approval in accordance with Paragraph 4 fully developed, complete and up-to-date Security Management Plan which shall comply with the requirements of Paragraph 4.2.

The Security Management Plan shall:

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

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

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

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

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

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

demonstrate that the Supplier's approach to delivery of the Deliverables has minimised the Buyer and Supplier effort required to comply with this Schedule through consideration of available, appropriate and practicable

pan-government accredited services (for example, 'platform as a service' offering from the G-Cloud catalogue);

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

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

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

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

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

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

## Amendment of the ISMS and Security Management Plan

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

emerging changes in Good Industry Practice;

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

any new perceived or changed security threats;

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

any new perceived or changed security threats; and any

reasonable change in requirement requested by the Buyer.

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

suggested improvements to the effectiveness of the ISMS;

updates to the risk assessments;

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

suggested improvements in measuring the effectiveness of controls.

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

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

## Security Testing

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

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

Without prejudice to any other right of audit or access granted to the Buyer pursuant to this Contract, the Buyer and/or its authorised representatives shall be entitled, at any time upon giving reasonable notice to the Supplier, to carry out such tests (including

penetration tests) as it may deem necessary in relation to the ISMS and the Supplier's compliance with the ISMS and the Security Management Plan. The Buyer may notify the Supplier of the results of such tests after completion of each such test. If any such Buyer's test adversely affects the Supplier's ability to deliver the Deliverables so as to meet the KPIs, the Supplier shall be granted relief against any resultant under-performance for the period of the Buyer's test.

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

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

## Complying with the ISMS

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

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

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

## Security Breach

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

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

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

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

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

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

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

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

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

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

## Vulnerabilities and fixing them

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

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

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

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

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

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

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

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

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

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

is agreed with the Buyer in writing.

The Supplier shall:

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

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

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

pro-actively scan the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) for vulnerable components and address discovered vulnerabilities through the processes described in the ISMS as developed under Paragraph 3.3.5;

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

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

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

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

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

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

# Part B – Annex 1:

# Baseline security requirements

## Handling Classified information

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

## End user devices

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

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

## Data Processing, Storage, Management and Destruction

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

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

The Supplier shall:

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

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

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

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

## Ensuring secure communications

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

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

## Security by design

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

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

## Security of Supplier Staff

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

The Supplier shall agree on a case by case basis Supplier Staff roles which require specific government clearances (such as 'SC') including system administrators with privileged access to IT systems which store or process Government Data.

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

All Supplier Staff that have the ability to access Government Data or systems holding Government Data shall undergo regular training on secure information management

principles. Unless otherwise agreed with the Buyer in writing, this training must be undertaken annually.

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

## Restricting and monitoring access

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

## Audit

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

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

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

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

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

# Part B – Annex 2 - Security Management Plan

[ ]

# Call-Off Schedule 10 (Exit Management)

## 1. Definitions

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

| | |
|---|---|
| **"Exclusive Assets"** | 1 Supplier Assets used exclusively by the Supplier the provision of the Deliverables; |
| **"Exit Information"** | 2 has the meaning given to it in Paragraph 3.1 of this Schedule; |
| **"Exit Manager"** | 3 the person appointed by each Party to manage their respective obligations under this Schedule; |
| **“Exit Plan”** | 4 the plan produced and updated by the Supplier during the Initial Period in accordance with Paragraph 4 of this Schedule; |
| **"Net Book Value"** | 5 the current net book value of the relevant Supplier Asset(s) calculated in accordance with the Framework Tender or Call-Off Tender (if stated) or (if not stated) the depreciation policy of the Supplier (which the Supplier shall ensure is in accordance with Good Industry Practice); |
| **"Non-Exclusive Assets"** | 6 those Supplier Assets used by the Supplier in connection with the Deliverables but which are also used by the Supplier for other purposes; |
| **"Registers"** | 7 the register and configuration database referred to in Paragraph 2.2 of this Schedule; |
| **"Replacement Goods"** | 8 any goods which are substantially similar to any of the Goods and which the Buyer receives in substitution for any of the Goods following the End Date, whether those goods are provided by the Buyer internally and/or by any third party; |
| **"Replacement Services"** | 9 any services which are substantially similar to any of the Services and which the Buyer receives in substitution for any of the Services following the End Date, whether those goods are provided by the Buyer internally and/or by any third party; |

| | | |
|---|---|---|
| **"Termination Assistance"** | 10 | the activities to be performed by the Supplier pursuant to the Exit Plan, and other assistance required by the Buyer pursuant to the Termination Assistance Notice; |
| **"Termination Assistance Notice"** | 11 | has the meaning given to it in Paragraph 5.1 of this Schedule; |
| **"Termination Assistance Period"** | 12 | the period specified in a Termination Assistance Notice for which the Supplier is required to provide the Termination Assistance as such period may be extended pursuant to Paragraph 5.2 of this Schedule; |
| **"Transferable Assets"** | 13 | Exclusive Assets which are capable of legal transfer to the Buyer; |
| **"Transferable Contracts"** | 14 | Sub-Contracts, licences for Supplier's Software, licences for Third Party Software or other agreements which are necessary to enable the Buyer or any Replacement Supplier to provide the Deliverables or the Replacement Goods and/or Replacement Services, including in relation to licences all relevant Documentation; |
| **"Transferring Assets"** | 15 | has the meaning given to it in Paragraph 8.2.1 of this Schedule; |
| **"Transferring Contracts"** | 16 | has the meaning given to it in Paragraph 8.2.3 of this Schedule. |

## 2. Supplier must always be prepared for contract exit

2.1 The Supplier shall within 30 days from the Start Date provide to the Buyer a copy of its depreciation policy to be used for the purposes of calculating Net Book Value.

2.2 During the Contract Period, the Supplier shall promptly:

2.2.1 create and maintain a detailed register of all Supplier Assets (including description, condition, location and details of ownership and status as either Exclusive Assets or Non-Exclusive Assets and Net Book Value) and Sub-contracts and other relevant agreements required in connection with the Deliverables; and

2.2.2 create and maintain a configuration database detailing the technical infrastructure and operating procedures through which the Supplier provides the Deliverables

("**Registers**").

2.3 The Supplier shall:

2.3.1 ensure that all Exclusive Assets listed in the Registers are clearly physically identified as such; and

2.3.2 procure that all licences for Third Party Software and all Sub-Contracts shall be assignable and/or capable of novation (at no cost or restriction to the Buyer) at the request of the Buyer to the Buyer (and/or its nominee) and/or any Replacement Supplier upon the Supplier ceasing to provide the Deliverables (or part of them) and if the Supplier is unable to do so then the Supplier shall promptly notify the Buyer and the Buyer may require the Supplier to procure an alternative Subcontractor or provider of Deliverables.

2.4 Each Party shall appoint an Exit Manager within three (3) Months of the Start Date. The Parties' Exit Managers will liaise with one another in relation to all issues relevant to the expiry or termination of this Contract.

## 3. Assisting re-competition for Deliverables

3.1 The Supplier shall, on reasonable notice, provide to the Buyer and/or its potential Replacement Suppliers (subject to the potential Replacement Suppliers entering into reasonable written confidentiality undertakings), such information (including any access) as the Buyer shall reasonably require in order to facilitate the preparation by the Buyer of any invitation to tender and/or to facilitate any potential Replacement Suppliers undertaking due diligence (the "**Exit Information**").

3.2 The Supplier acknowledges that the Buyer may disclose the Supplier's Confidential Information (excluding the Supplier's or its Subcontractors' prices or costs) to an actual or prospective Replacement Supplier to the extent that such disclosure is necessary in connection with such engagement.

3.3 The Supplier shall provide complete updates of the Exit Information on an as-requested basis as soon as reasonably practicable and notify the Buyer within five (5) Working Days of any material change to the Exit Information which may adversely impact upon the provision of any Deliverables (and shall consult the Buyer in relation to any such changes).

3.4 The Exit Information shall be accurate and complete in all material respects and shall be sufficient to enable a third party to prepare an informed offer for those Deliverables; and not be disadvantaged in any procurement process compared to the Supplier.

## 4. Exit Plan

4.1 The Supplier shall, within three (3) Months after the Start Date, deliver to the Buyer an Exit Plan which complies with the requirements set out in Paragraph 4.3 of this Schedule and is otherwise reasonably satisfactory to the Buyer.

4.2 The Parties shall use reasonable endeavours to agree the contents of the Exit Plan. If the Parties are unable to agree the contents of the Exit Plan within twenty (20) Working Days of the latest date for its submission pursuant to Paragraph 4.1, then such Dispute shall be resolved in accordance with the Dispute Resolution Procedure.

4.3 The Exit Plan shall set out, as a minimum:

4.3.1 a detailed description of both the transfer and cessation processes, including a timetable;

4.3.2 how the Deliverables will transfer to the Replacement Supplier and/or the Buyer;

4.3.3 details of any contracts which will be available for transfer to the Buyer and/or the Replacement Supplier upon the Expiry Date together with any reasonable costs required to effect such transfer;

4.3.4 proposals for the training of key members of the Replacement Supplier's staff in connection with the continuation of the provision of the Deliverables following the Expiry Date;

4.3.5 proposals for providing the Buyer or a Replacement Supplier copies of all documentation relating to the use and operation of the Deliverables and required for their continued use;

4.3.6 proposals for the assignment or novation of all services utilised by the Supplier in connection with the supply of the Deliverables;

4.3.7 proposals for the identification and return of all Buyer Property in the possession of and/or control of the Supplier or any third party;

4.3.8 proposals for the disposal of any redundant Deliverables and materials;

4.3.9 how the Supplier will ensure that there is no disruption to or degradation of the Deliverables during the Termination Assistance Period; and

4.3.10 any other information or assistance reasonably required by the Buyer or a Replacement Supplier.

4.4 The Supplier shall:

4.4.1 maintain and update the Exit Plan (and risk management plan) no less frequently than:

(a) every six (6) months throughout the Contract Period; and

(b) no later than twenty (20) Working Days after a request from the Buyer for an up-to-date copy of the Exit Plan;

(c) as soon as reasonably possible following a Termination Assistance Notice, and in any event no later than ten (10) Working Days after the date of the Termination Assistance Notice;

(d) as soon as reasonably possible following, and in any event no later than twenty (20) Working Days following, any material change to the Deliverables (including all changes under the Variation Procedure); and

4.4.2 jointly review and verify the Exit Plan if required by the Buyer and promptly correct any identified failures.

4.5 Only if (by notification to the Supplier in writing) the Buyer agrees with a draft Exit Plan provided by the Supplier under Paragraph 4.2 or 4.4 (as the context requires), shall that draft become the Exit Plan for this Contract.

4.6 A version of an Exit Plan agreed between the parties shall not be superseded by any draft submitted by the Supplier.

## 5. Termination Assistance

5.1 The Buyer shall be entitled to require the provision of Termination Assistance at any time during the Contract Period by giving written notice to the Supplier (a **"Termination Assistance Notice"**) at least four (4) Months prior to the Expiry Date or as soon as reasonably practicable (but in any event, not later than one (1) Month) following the service by either Party of a Termination Notice. The Termination Assistance Notice shall specify:

5.1.1 the nature of the Termination Assistance required; and

5.1.2 the start date and initial period during which it is anticipated that Termination Assistance will be required, which shall continue no longer than twelve (12) Months after the End Date.

5.2 The Buyer shall have an option to extend the Termination Assistance Period beyond the initial period specified in the Termination Assistance Notice in one or more extensions, in each case provided that:

5.2.1 no such extension shall extend the Termination Assistance Period beyond the date twelve (12) Months after the End Date; and

5.2.2 the Buyer shall notify the Supplier of any such extension no later than twenty (20) Working Days prior to the date on which the Termination Assistance Period is otherwise due to expire.

5.3 The Buyer shall have the right to terminate its requirement for Termination Assistance by serving not less than (20) Working Days' written notice upon the Supplier.

5.4 In the event that Termination Assistance is required by the Buyer but at the relevant time the parties are still agreeing an update to the Exit Plan pursuant to Paragraph 4, the Supplier will provide the Termination Assistance in good faith and in accordance with the principles in this Schedule and the last Buyer approved version of the Exit Plan (insofar as it still applies).

## 6. Termination Assistance Period

6.1 Throughout the Termination Assistance Period the Supplier shall:

6.1.1 continue to provide the Deliverables (as applicable) and otherwise perform its obligations under this Contract and, if required by the Buyer, provide the Termination Assistance;

6.1.2 provide to the Buyer and/or its Replacement Supplier any reasonable assistance and/or access requested by the Buyer and/or its Replacement Supplier including assistance and/or access to facilitate the orderly transfer of responsibility for and conduct of the Deliverables to the Buyer and/or its Replacement Supplier;

6.1.3 use all reasonable endeavours to reallocate resources to provide such assistance without additional costs to the Buyer;

6.1.4 subject to Paragraph 6.3, provide the Deliverables and the Termination Assistance at no detriment to the Performance Indicators (PI's) or Service Levels, the provision of the Management Information or any other reports nor to any other of the Supplier's obligations under this Contract;

6.1.5 at the Buyer's request and on reasonable notice, deliver up-to-date Registers to the Buyer;

6.1.6 seek the Buyer's prior written consent to access any Buyer Premises from which the de-installation or removal of Supplier Assets is required.

6.2 If it is not possible for the Supplier to reallocate resources to provide such assistance as is referred to in Paragraph 6.1.2 without additional costs to the Buyer, any additional costs incurred by the Supplier in providing such reasonable assistance shall be subject to the Variation Procedure.

6.3 If the Supplier demonstrates to the Buyer's reasonable satisfaction that the provision of the Termination Assistance will have a material, unavoidable adverse effect on the Supplier's ability to meet one or more particular

Service Levels, the Parties shall vary the relevant Service Levels and/or the applicable Service Credits accordingly.

## 7. Obligations when the contract is terminated

7.1 The Supplier shall comply with all of its obligations contained in the Exit Plan.

7.2 Upon termination or expiry or at the end of the Termination Assistance Period (or earlier if this does not adversely affect the Supplier's performance of the Deliverables and the Termination Assistance), the Supplier shall:

7.2.1 vacate any Buyer Premises;

7.2.2 remove the Supplier Equipment together with any other materials used by the Supplier to supply the Deliverables and shall leave the Sites in a clean, safe and tidy condition. The Supplier is solely responsible for making good any damage to the Sites or any objects contained thereon, other than fair wear and tear, which is caused by the Supplier;

7.2.3 provide access during normal working hours to the Buyer and/or the Replacement Supplier for up to twelve (12) Months after expiry or termination to:

(a) such information relating to the Deliverables as remains in the possession or control of the Supplier; and

(b) such members of the Supplier Staff as have been involved in the design, development and provision of the Deliverables and who are still employed by the Supplier, provided that the Buyer and/or the Replacement Supplier shall pay the reasonable costs of the Supplier actually incurred in responding to such requests for access.

7.3 Except where this Contract provides otherwise, all licences, leases and authorisations granted by the Buyer to the Supplier in relation to the Deliverables shall be terminated with effect from the end of the Termination Assistance Period.

## 8. Assets, Sub-contracts and Software

8.1 Following notice of termination of this Contract and during the Termination Assistance Period, the Supplier shall not, without the Buyer's prior written consent:

8.1.1 terminate, enter into or vary any Sub-contract or licence for any software in connection with the Deliverables; or

8.1.2 (subject to normal maintenance requirements) make material modifications to, or dispose of, any existing Supplier Assets or acquire any new Supplier Assets.

8.2 Within twenty (20) Working Days of receipt of the up-to-date Registers provided by the Supplier, the Buyer shall notify the Supplier setting out:

8.2.1 which, if any, of the Transferable Assets the Buyer requires to be transferred to the Buyer and/or the Replacement Supplier ("**Transferring Assets**");

8.2.2 which, if any, of:

(a) the Exclusive Assets that are not Transferable Assets; and

(b) the Non-Exclusive Assets,

the Buyer and/or the Replacement Supplier requires the continued use of; and

8.2.3 which, if any, of Transferable Contracts the Buyer requires to be assigned or novated to the Buyer and/or the Replacement Supplier (the **"Transferring Contracts"**),

in order for the Buyer and/or its Replacement Supplier to provide the Deliverables from the expiry of the Termination Assistance Period. The Supplier shall provide all reasonable assistance required by the Buyer and/or its Replacement Supplier to enable it to determine which Transferable Assets and Transferable Contracts are required to provide the Deliverables or the Replacement Goods and/or Replacement Services.

8.3 With effect from the expiry of the Termination Assistance Period, the Supplier shall sell the Transferring Assets to the Buyer and/or the Replacement Supplier for their Net Book Value less any amount already paid for them through the Charges.

8.4 Risk in the Transferring Assets shall pass to the Buyer or the Replacement Supplier (as appropriate) at the end of the Termination Assistance Period and title shall pass on payment for them.

8.5 Where the Buyer and/or the Replacement Supplier requires continued use of any Exclusive Assets that are not Transferable Assets or any Non-Exclusive Assets, the Supplier shall as soon as reasonably practicable:

8.5.1 procure a non-exclusive, perpetual, royalty-free licence for the Buyer and/or the Replacement Supplier to use such assets (with a right of sub-licence or assignment on the same terms); or failing which

8.5.2 procure a suitable alternative to such assets, the Buyer or the Replacement Supplier to bear the reasonable proven costs of procuring the same.

8.6 The Supplier shall as soon as reasonably practicable assign or procure the novation of the Transferring Contracts to the Buyer and/or the Replacement Supplier. The Supplier shall execute such documents and provide such

other assistance as the Buyer reasonably requires to effect this novation or assignment.

8.7 The Buyer shall:

8.7.1 accept assignments from the Supplier or join with the Supplier in procuring a novation of each Transferring Contract; and

8.7.2 once a Transferring Contract is novated or assigned to the Buyer and/or the Replacement Supplier, discharge all the obligations and liabilities created by or arising under that Transferring Contract and exercise its rights arising under that Transferring Contract, or as applicable, procure that the Replacement Supplier does the same.

8.8 The Supplier shall hold any Transferring Contracts on trust for the Buyer until the transfer of the relevant Transferring Contract to the Buyer and/or the Replacement Supplier has taken place.

8.9 The Supplier shall indemnify the Buyer (and/or the Replacement Supplier, as applicable) against each loss, liability and cost arising out of any claims made by a counterparty to a Transferring Contract which is assigned or novated to the Buyer (and/or Replacement Supplier) pursuant to Paragraph 8.6 in relation to any matters arising prior to the date of assignment or novation of such Transferring Contract. Clause 19 (Other people's rights in this contract) shall not apply to this Paragraph 8.9 which is intended to be enforceable by Third Parties Beneficiaries by virtue of the CRTPA.

## 9. No charges

9.1 Unless otherwise stated, the Buyer shall not be obliged to pay for costs incurred by the Supplier in relation to its compliance with this Schedule.

## 10. Dividing the bills

10.1 All outgoings, expenses, rents, royalties and other periodical payments receivable in respect of the Transferring Assets and Transferring Contracts shall be apportioned between the Buyer and/or the Replacement and the Supplier as follows:

10.1.1 the amounts shall be annualised and divided by 365 to reach a daily rate;

10.1.2 the Buyer or Replacement Supplier (as applicable) shall be responsible for or entitled to (as the case may be) that part of the value of the invoice pro rata to the number of complete days following the transfer, multiplied by the daily rate; and

10.1.3 the Supplier shall be responsible for or entitled to (as the case may be) the rest of the invoice.

# Call-Off Schedule 13 (Implementation Plan and Testing)

## Part A - Implementation

### 1. Definitions

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

| | |
|---|---|
| **"Delay"** | a) a delay in the Achievement of a Milestone by its Milestone Date; or<br>b) a delay in the design, development, testing or implementation of a Deliverable by the relevant date set out in the Implementation Plan; |
| **"Deliverable Item"** | 1 an item or feature in the supply of the Deliverables delivered or to be delivered by the Supplier at or before a Milestone Date listed in the Implementation Plan; |
| **"Milestone Payment"** | 2 a payment identified in the Implementation Plan to be made following the issue of a Satisfaction Certificate in respect of Achievement of the relevant Milestone; |
| **Implementation Period"** | 3 has the meaning given to it in Paragraph 7.1; |

### 3. Agreeing and following the Implementation Plan

2.1 A draft of the Implementation Plan is set out in the Annex to this Schedule. The Supplier shall provide a further draft Implementation Plan 30 days after the Call-Off Contract Start Date.

2.2 The draft Implementation Plan:

2.2.1 must contain information at the level of detail necessary to manage the implementation stage effectively and as the Buyer may otherwise require; and

2.2.2 it shall take account of all dependencies known to, or which should reasonably be known to, the Supplier.

2.3 Following receipt of the draft Implementation Plan from the Supplier, the Parties shall use reasonable endeavours to agree the contents of the Implementation Plan. If the Parties are unable to agree the contents of the

Implementation Plan within twenty (20) Working Days of its submission, then such Dispute shall be resolved in accordance with the Dispute Resolution Procedure.

2.4 The Supplier shall provide each of the Deliverable Items identified in the Implementation Plan by the date assigned to that Deliverable Item in the Implementation Plan so as to ensure that each Milestone identified in the Implementation Plan is Achieved on or before its Milestone Date.

2.5 The Supplier shall monitor its performance against the Implementation Plan and Milestones (if any) and report to the Buyer on such performance.

## 6. Reviewing and changing the Implementation Plan

3.1 Subject to Paragraph 4.3, the Supplier shall keep the Implementation Plan under review in accordance with the Buyer's instructions and ensure that it is updated on a regular basis.

3.2 The Buyer shall have the right to require the Supplier to include any reasonable changes or provisions in each version of the Implementation Plan.

3.3 Changes to any Milestones, Milestone Payments and Delay Payments shall only be made in accordance with the Variation Procedure.

3.4 Time in relation to compliance with the Implementation Plan shall be of the essence and failure of the Supplier to comply with the Implementation Plan shall be a material Default.

## 7. Security requirements before the Start Date

4.1 The Supplier shall note that it is incumbent upon them to understand the lead-in period for security clearances and ensure that all Supplier Staff have the necessary security clearance in place before the Call-Off Start Date. The Supplier shall ensure that this is reflected in their Implementation Plans.

4.2 The Supplier shall ensure that all Supplier Staff and Subcontractors do not access the Buyer's IT systems, or any IT systems linked to the Buyer, unless they have satisfied the Buyer's security requirements.

4.3 The Supplier shall be responsible for providing all necessary information to the Buyer to facilitate security clearances for Supplier Staff and Subcontractors in accordance with the Buyer's requirements.

4.4 The Supplier shall provide the names of all Supplier Staff and Subcontractors and inform the Buyer of any alterations and additions as they take place throughout the Call-Off Contract.

4.5 The Supplier shall ensure that all Supplier Staff and Subcontractors requiring access to the Buyer Premises have the appropriate security clearance. It is the Supplier's responsibility to establish whether or not the level of clearance will be sufficient for access. Unless prior approval has been received from the Buyer, the Supplier shall be responsible for meeting the costs associated with the provision of security cleared escort services.

4.6 If a property requires Supplier Staff or Subcontractors to be accompanied by the Buyer's Authorised Representative, the Buyer must be given reasonable notice of such a requirement, except in the case of emergency access.

## 4. What to do if there is a Delay

5.1 If the Supplier becomes aware that there is, or there is reasonably likely to be, a Delay under this Contract it shall:

5.1.1 notify the Buyer as soon as practically possible and no later than within two (2) Working Days from becoming aware of the Delay or anticipated Delay;

5.1.2 include in its notification an explanation of the actual or anticipated impact of the Delay;

5.1.3 comply with the Buyer's instructions in order to address the impact of the Delay or anticipated Delay; and

5.1.4 use all reasonable endeavours to eliminate or mitigate the consequences of any Delay or anticipated Delay.

## 5. Compensation for a Delay

6.1 If Delay Payments have been included in the Implementation Plan and a Milestone has not been achieved by the relevant Milestone Date, the Supplier shall pay to the Buyer such Delay Payments (calculated as set out by the Buyer in the Implementation Plan) and the following provisions shall apply:

6.1.1 the Supplier acknowledges and agrees that any Delay Payment is a price adjustment and not an estimate of the Loss that may be suffered by the Buyer as a result of the Supplier's failure to Achieve the corresponding Milestone;

6.1.2 Delay Payments shall be the Buyer's exclusive financial remedy for the Supplier's failure to Achieve a Milestone by its Milestone Date except where:

(a) the Buyer is entitled to or does terminate this Contract pursuant to Clause 10.4 (When CCS or the Buyer can end this contract); or

(b) the delay exceeds the number of days (the "**Delay Period Limit**") specified in the Implementation Plan commencing on the relevant Milestone Date;

6.1.3 the Delay Payments will accrue on a daily basis from the relevant Milestone Date until the date when the Milestone is Achieved;

6.1.4 no payment or other act or omission of the Buyer shall in any way affect the rights of the Buyer to recover the Delay Payments or be deemed to be a waiver of the right of the Buyer to recover any such damages; and

6.1.5 Delay Payments shall not be subject to or count towards any limitation on liability set out in Clause 11 (How much you can be held responsible for).

## 7. Implementation Plan

7.1 The Implementation Period will be a [six (6)] Month period.

7.2 During the Implementation Period, the incumbent supplier shall retain full responsibility for all existing services until the Call-Off Start Date or as otherwise formally agreed with the Buyer. The Supplier's full service obligations shall formally be assumed on the Call-Off Start Date as set out in Order Form.

7.3 In accordance with the Implementation Plan, the Supplier shall:

7.3.1 work cooperatively and in partnership with the Buyer, incumbent supplier, and other Framework Supplier(s), where applicable, to understand the scope of Services to ensure a mutually beneficial handover of the Services;

7.3.2 work with the incumbent supplier and Buyer to assess the scope of the Services and prepare a plan which demonstrates how they will mobilise the Services;

7.3.3 liaise with the incumbent Supplier to enable the full completion of the Implementation Period activities; and

7.3.4 produce a Implementation Plan, to be agreed by the Buyer, for carrying out the requirements within the Implementation Period including, key Milestones and dependencies.

7.4 The Implementation Plan will include detail stating:

7.4.1 how the Supplier will work with the incumbent Supplier and the Buyer Authorised Representative to capture and load up information such as asset data ; and

7.4.2 a communications plan, to be produced and implemented by the Supplier, but to be agreed with the Buyer, including the frequency,

responsibility for and nature of communication with the Buyer and end users of the Services.

7.5 In addition, the Supplier shall:

7.5.1 appoint a Supplier Authorised Representative who shall be responsible for the management of the Implementation Period, to ensure that the Implementation Period is planned and resourced adequately, and who will act as a point of contact for the Buyer;

7.5.2 mobilise all the Services specified in the Specification within the Call-Off Contract;

7.5.3 produce a Implementation Plan report for each Buyer Premises to encompass programmes that will fulfil all the Buyer's obligations to landlords and other tenants:

(a) the format of reports and programmes shall be in accordance with the Buyer's requirements and particular attention shall be paid to establishing the operating requirements of the occupiers when preparing these programmes which are subject to the Buyer's approval; and

(b) the Parties shall use reasonable endeavours to agree the contents of the report but if the Parties are unable to agree the contents within twenty (20) Working Days of its submission by the Supplier to the Buyer, then such Dispute shall be resolved in accordance with the Dispute Resolution Procedure.

7.5.4 manage and report progress against the Implementation Plan;

7.5.5 construct and maintain a Implementation risk and issue register in conjunction with the Buyer detailing how risks and issues will be effectively communicated to the Buyer in order to mitigate them;

7.5.6 attend progress meetings (frequency of such meetings shall be as set out in the Order Form) in accordance with the Buyer's requirements during the Implementation Period. Implementation meetings shall be chaired by the Buyer and all meeting minutes shall be kept and published by the Supplier; and

7.5.7 ensure that all risks associated with the Implementation Period are minimised to ensure a seamless change of control between incumbent provider and the Supplier.

**Annex 1: Implementation Plan**

The Implementation Plan is set out below and the Milestones to be Achieved are identified below:

| Milestone | Deliverable Items | Duration | Milestone Date | Buyer Responsibilities | Milestone Payments | Delay Payments |
|---|---|---|---|---|---|---|
| [ ] | [ ] | [ ] | [ ] | [ ] | [ ] | [ ] |

The Milestones will be Achieved in accordance with this Call-Off Schedule 13: (Implementation Plan and Testing)

For the purposes of Paragraph 9.1.2 the Delay Period Limit shall be **[insert number of days].**

# Part B - Testing

## 1. Definitions

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

| | |
|---|---|
| **"Component"** | 4 any constituent parts of the Deliverables; |
| **"Material Test Issue"** | 5 a Test Issue of Severity Level 1 or Severity Level 2; |
| **"Satisfaction Certificate"** | 6 a certificate materially in the form of the document contained in Annex 2 issued by the Buyer when a Deliverable and/or Milestone has satisfied its relevant Test Success Criteria; |
| **"Severity Level"** | 7 the level of severity of a Test Issue, the criteria for which are described in Annex 1; |
| **"Test Issue Management Log"** | 8 a log for the recording of Test Issues as described further in Paragraph 8.1 of this Schedule; |
| **"Test Issue Threshold"** | 9 in relation to the Tests applicable to a Milestone, a maximum number of Severity Level 3, Severity Level 4 and Severity Level 5 Test Issues as set out in the relevant Test Plan; |
| **"Test Reports"** | 10 the reports to be produced by the Supplier setting out the results of Tests; |
| **"Test Specification"** | 11 the specification that sets out how Tests will demonstrate that the Test Success Criteria have been satisfied, as |

| | | |
|---|---|---|
| | | described in more detail in Paragraph 6.2 of this Schedule; |
| **"Test Strategy"** | 12 | a strategy for the conduct of Testing as described further in Paragraph 3.2 of this Schedule; |
| **"Test Success Criteria"** | 13 | in relation to a Test, the test success criteria for that Test as referred to in Paragraph 5 of this Schedule; |
| **"Test Witness"** | 14 | any person appointed by the Buyer pursuant to Paragraph 9 of this Schedule; and |
| **"Testing Procedures"** | 15 | the applicable testing procedures and Test Success Criteria set out in this Schedule. |

## 2. How testing should work

2.1 All Tests conducted by the Supplier shall be conducted in accordance with the Test Strategy, Test Specification and the Test Plan.

2.2 The Supplier shall not submit any Deliverable for Testing:

2.2.1 unless the Supplier is reasonably confident that it will satisfy the relevant Test Success Criteria;

2.2.2 until the Buyer has issued a Satisfaction Certificate in respect of any prior, dependant Deliverable(s); and

2.2.3 until the Parties have agreed the Test Plan and the Test Specification relating to the relevant Deliverable(s).

2.3 The Supplier shall use reasonable endeavours to submit each Deliverable for Testing or re-Testing by or before the date set out in the Implementation Plan for the commencement of Testing in respect of the relevant Deliverable.

2.4 Prior to the issue of a Satisfaction Certificate, the Buyer shall be entitled to review the relevant Test Reports and the Test Issue Management Log.

## 3. Planning for testing

3.1 The Supplier shall develop the final Test Strategy as soon as practicable after the Start Date but in any case no later than twenty (20) Working Days after the Start Date.

3.2 The final Test Strategy shall include:

3.2.1 an overview of how Testing will be conducted in relation to the Implementation Plan;

3.2.2 the process to be used to capture and record Test results and the categorisation of Test Issues;

3.2.3 the procedure to be followed should a Deliverable fail a Test, fail to satisfy the Test Success Criteria or where the Testing of a Deliverable produces unexpected results, including a procedure for the resolution of Test Issues;

3.2.4 the procedure to be followed to sign off each Test;

3.2.5 the process for the production and maintenance of Test Reports and a sample plan for the resolution of Test Issues;

3.2.6 the names and contact details of the Buyer and the Supplier's Test representatives;

3.2.7 a high level identification of the resources required for Testing including Buyer and/or third party involvement in the conduct of the Tests;

3.2.8 the technical environments required to support the Tests; and

3.2.9 the procedure for managing the configuration of the Test environments.

## 4. Preparing for Testing

4.1 The Supplier shall develop Test Plans and submit these for Approval as soon as practicable but in any case no later than twenty (20) Working Days prior to the start date for the relevant Testing as specified in the Implementation Plan.

4.2 Each Test Plan shall include as a minimum:

4.2.1 the relevant Test definition and the purpose of the Test, the Milestone to which it relates, the requirements being Tested and, for each Test, the specific Test Success Criteria to be satisfied; and

4.2.2a detailed procedure for the Tests to be carried out.

4.3 The Buyer shall not unreasonably withhold or delay its approval of the Test Plan provided that the Supplier shall implement any reasonable requirements of the Buyer in the Test Plan.

## 5. Passing Testing

5.1 The Test Success Criteria for all Tests shall be agreed between the Parties as part of the relevant Test Plan pursuant to Paragraph 4.

## 6. How Deliverables will be tested

6.1 Following approval of a Test Plan, the Supplier shall develop the Test Specification for the relevant Deliverables as soon as reasonably practicable and in any event at least 10 Working Days prior to the start of the relevant Testing (as specified in the Implementation Plan).

6.2 Each Test Specification shall include as a minimum:

6.2.1the specification of the Test data, including its source, scope, volume and management, a request (if applicable) for relevant Test data to be provided by the Buyer and the extent to which it is equivalent to live operational data;

6.2.2 a plan to make the resources available for Testing;

6.2.3 Test scripts;

6.2.4Test pre-requisites and the mechanism for measuring them; and

6.2.5 expected Test results, including:

(a) a mechanism to be used to capture and record Test results; and

(b) a method to process the Test results to establish their content.

## 7. Performing the tests

7.1 Before submitting any Deliverables for Testing the Supplier shall subject the relevant Deliverables to its own internal quality control measures.

7.2 The Supplier shall manage the progress of Testing in accordance with the relevant Test Plan and shall carry out the Tests in accordance with the

relevant Test Specification. Tests may be witnessed by the Test Witnesses in accordance with Paragraph 9.3.

7.3 The Supplier shall notify the Buyer at least 10 Working Days in advance of the date, time and location of the relevant Tests and the Buyer shall ensure that the Test Witnesses attend the Tests.

7.4 The Buyer may raise and close Test Issues during the Test witnessing process.

7.5 The Supplier shall provide to the Buyer in relation to each Test:

7.5.1a draft Test Report not less than 2 Working Days prior to the date on which the Test is planned to end; and

7.5.2the final Test Report within 5 Working Days of completion of Testing.

7.6 Each Test Report shall provide a full report on the Testing conducted in respect of the relevant Deliverables, including:

7.6.1 an overview of the Testing conducted;

7.6.2 identification of the relevant Test Success Criteria that have/have not been satisfied together with the Supplier's explanation of why any criteria have not been met;

7.6.3the Tests that were not completed together with the Supplier's explanation of why those Tests were not completed;

7.6.4the Test Success Criteria that were satisfied, not satisfied or which were not tested, and any other relevant categories, in each case grouped by Severity Level in accordance with Paragraph 8.1; and

7.6.5the specification for any hardware and software used throughout Testing and any changes that were applied to that hardware and/or software during Testing.

7.7 When the Supplier has completed a Milestone it shall submit any Deliverables relating to that Milestone for Testing.

7.8 Each party shall bear its own costs in respect of the Testing. However, if a Milestone is not Achieved the Buyer shall be entitled to recover from the Supplier, any reasonable additional costs it may incur as a direct result of further review or re-Testing of a Milestone.

7.9 If the Supplier successfully completes the requisite Tests, the Buyer shall issue a Satisfaction Certificate as soon as reasonably practical following such successful completion. Notwithstanding the issuing of any Satisfaction

Certificate, the Supplier shall remain solely responsible for ensuring that the Deliverables are implemented in accordance with this Contract.

## 8. Discovering Problems

8.1 Where a Test Report identifies a Test Issue, the Parties shall agree the classification of the Test Issue using the criteria specified in Annex 1 and the Test Issue Management Log maintained by the Supplier shall log Test Issues reflecting the Severity Level allocated to each Test Issue.

8.2 The Supplier shall be responsible for maintaining the Test Issue Management Log and for ensuring that its contents accurately represent the current status of each Test Issue at all relevant times. The Supplier shall make the Test Issue Management Log available to the Buyer upon request.

8.3 The Buyer shall confirm the classification of any Test Issue unresolved at the end of a Test in consultation with the Supplier. If the Parties are unable to agree the classification of any unresolved Test Issue, the Dispute shall be dealt with in accordance with the Dispute Resolution Procedure using the Expedited Dispute Timetable.

## 9. Test witnessing

9.1 The Buyer may, in its sole discretion, require the attendance at any Test of one or more Test Witnesses selected by the Buyer, each of whom shall have appropriate skills to fulfil the role of a Test Witness.

9.2 The Supplier shall give the Test Witnesses access to any documentation and Testing environments reasonably necessary and requested by the Test Witnesses to perform their role as a Test Witness in respect of the relevant Tests.

9.3 The Test Witnesses:

9.3.1 shall actively review the Test documentation;

9.3.2 will attend and engage in the performance of the Tests on behalf of the Buyer so as to enable the Buyer to gain an informed view of whether a Test Issue may be closed or whether the relevant element of the Test should be re-Tested;

9.3.3 shall not be involved in the execution of any Test;

9.3.4 shall be required to verify that the Supplier conducted the Tests in accordance with the Test Success Criteria and the relevant Test Plan and Test Specification;

9.3.5 may produce and deliver their own, independent reports on Testing, which may be used by the Buyer to assess whether the Tests have been Achieved;

9.3.6 may raise Test Issues on the Test Issue Management Log in respect of any Testing; and

9.4 may require the Supplier to demonstrate the modifications made to any defective Deliverable before a Test Issue is closed.

## 10. Auditing the quality of the test

10.1 The Buyer or an agent or contractor appointed by the Buyer may perform on-going quality audits in respect of any part of the Testing (each a "**Testing Quality Audit**") subject to the provisions set out in the agreed Quality Plan.

10.2 The Supplier shall allow sufficient time in the Test Plan to ensure that adequate responses to a Testing Quality Audit can be provided.

10.3 The Buyer will give the Supplier at least 5 Working Days' written notice of the Buyer's intention to undertake a Testing Quality Audit.

10.4 The Supplier shall provide all reasonable necessary assistance and access to all relevant documentation required by the Buyer to enable it to carry out the Testing Quality Audit.

10.5 If the Testing Quality Audit gives the Buyer concern in respect of the Testing Procedures or any Test, the Buyer shall prepare a written report for the Supplier detailing its concerns and the Supplier shall, within a reasonable timeframe, respond in writing to the Buyer's report.

10.6 In the event of an inadequate response to the written report from the Supplier, the Buyer (acting reasonably) may withhold a Satisfaction Certificate until the issues in the report have been addressed to the reasonable satisfaction of the Buyer.

## 11. Outcome of the testing

11.1 The Buyer will issue a Satisfaction Certificate when the Deliverables satisfy the Test Success Criteria in respect of that Test without any Test Issues.

11.2 If the Deliverables (or any relevant part) do not satisfy the Test Success Criteria then the Buyer shall notify the Supplier and:

11.2.1 the Buyer may issue a Satisfaction Certificate conditional upon the remediation of the Test Issues;

11.2.2 the Buyer may extend the Test Plan by such reasonable period or periods as the Parties may reasonably agree and require the Supplier to rectify the cause of the Test Issue and re-submit the Deliverables (or the relevant part) to Testing; or

11.2.3 where the failure to satisfy the Test Success Criteria results, or is likely to result, in the failure (in whole or in part) by the Supplier to meet a Milestone, then without prejudice to the Buyer's other rights and remedies, such failure shall constitute a material Default.

11.3 The Buyer shall be entitled, without prejudice to any other rights and remedies that it has under this Contract, to recover from the Supplier any reasonable additional costs it may incur as a direct result of further review or re-Testing which is required for the Test Success Criteria for that Deliverable to be satisfied.

11.4 The Buyer shall issue a Satisfaction Certificate in respect of a given Milestone as soon as is reasonably practicable following:

11.4.1 the issuing by the Buyer of Satisfaction Certificates and/or conditional Satisfaction Certificates in respect of all Deliverables related to that Milestone which are due to be Tested; and

11.4.2 performance by the Supplier to the reasonable satisfaction of the Buyer of any other tasks identified in the Implementation Plan as associated with that Milestone.

11.5 The grant of a Satisfaction Certificate shall entitle the Supplier to the receipt of a payment in respect of that Milestone in accordance with the provisions of any Implementation Plan and Clause 4 (Pricing and payments).

11.6 If a Milestone is not Achieved, the Buyer shall promptly issue a report to the Supplier setting out the applicable Test Issues and any other reasons for the relevant Milestone not being Achieved.

11.7 If there are Test Issues but these do not exceed the Test Issues Threshold, then provided there are no Material Test Issues, the Buyer shall issue a Satisfaction Certificate.

11.8 If there is one or more Material Test Issue(s), the Buyer shall refuse to issue a Satisfaction Certificate and, without prejudice to the Buyer's other rights and remedies, such failure shall constitute a material Default.

11.9 If there are Test Issues which exceed the Test Issues Threshold but there are no Material Test Issues, the Buyer may at its discretion (without waiving any rights in relation to the other options) choose to issue a Satisfaction

Certificate conditional on the remediation of the Test Issues in accordance with an agreed Rectification Plan provided that:

11.9.1 any Rectification Plan shall be agreed before the issue of a conditional Satisfaction Certificate unless the Buyer agrees otherwise (in which case the Supplier shall submit a Rectification Plan for approval by the Buyer within 10 Working Days of receipt of the Buyer's report pursuant to Paragraph 10.5); and

11.9.2 where the Buyer issues a conditional Satisfaction Certificate, it may (but shall not be obliged to) revise the failed Milestone Date and any subsequent Milestone Date.

## 12. Risk

12.1 The issue of a Satisfaction Certificate and/or a conditional Satisfaction Certificate shall not:

12.1.1 operate to transfer any risk that the relevant Deliverable or Milestone is complete or will meet and/or satisfy the Buyer's requirements for that Deliverable or Milestone; or

12.1.2 affect the Buyer's right subsequently to reject all or any element of the Deliverables and/or any Milestone to which a Satisfaction Certificate relates.

# Annex 1: Test Issues – Severity Levels

### Severity 1 Error

This is an error that causes non-recoverable conditions, e.g. it is not possible to continue using a Component.

### Severity 2 Error

This is an error for which, as reasonably determined by the Buyer, there is no practicable workaround available, and which:

causes a Component to become unusable;

causes a lack of functionality, or unexpected functionality, that has an impact on the current Test; or

has an adverse impact on any other Component(s) or any other area of the Deliverables;

### Severity 3 Error

This is an error which:

causes a Component to become unusable;

causes a lack of functionality, or unexpected functionality, but which does not impact on the current Test; or

has an impact on any other Component(s) or any other area of the Deliverables;

but for which, as reasonably determined by the Buyer, there is a practicable workaround available;

### Severity 4 Error

This is an error which causes incorrect functionality of a Component or process, but for which there is a simple, Component based, workaround, and which has no impact on the current Test, or other areas of the Deliverables.

### Severity 5 Error

This is an error that causes a minor problem, for which no workaround is required, and which has no impact on the current Test, or other areas of the Deliverables.

# Annex 2: Satisfaction Certificate

To: [insert name of Supplier]

From: [insert name of Buyer]

[insert Date dd/mm/yyyy]

Dear Sirs,

**Satisfaction Certificate**

Deliverable/Milestone(s): [Insert relevant description of the agreed Deliverables/Milestones].

We refer to the agreement (**"Call-Off Contract"**) [insert Call-Off Contract reference number] relating to the provision of the [insert description of the Deliverables] between the [*insert Buyer name*] (**"Buyer"**) and [*insert Supplier name*] (**"Supplier"**) dated [*insert Call-Off Start Date dd/mm/yyyy*].

The definitions for any capitalised terms in this certificate are as set out in the Call-Off Contract.

[We confirm that all the Deliverables relating to [insert relevant description of Deliverables/agreed Milestones and/or reference number(s) from the Implementation Plan] have been tested successfully in accordance with the Test Plan [or that a conditional Satisfaction Certificate has been issued in

respect of those Deliverables that have not satisfied the relevant Test Success Criteria].

[OR]

[This Satisfaction Certificate is granted on the condition that any Test Issues are remedied in accordance with the Rectification Plan attached to this certificate.]

[You may now issue an invoice in respect of the Milestone Payment associated with this Milestone in accordance with Clause 4 (Pricing and payments)].

Yours faithfully

[insert Name]

[insert Position]

acting on behalf of [insert name of Buyer]

# Call-Off Schedule 15 (Call-Off Contract Management)

## 1. Definitions

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

| | |
|---|---|
| **"Operational Board"** | the board established in accordance with paragraph 4.1 of this Schedule; |
| **"Project Manager"** | the manager appointed in accordance with paragraph 2.1 of this Schedule; |

## 2. Project Management

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

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

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

## 3. Role of the Supplier Contract Manager

3.1 The Supplier's Contract Manager's shall be:

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

**3.1.2** **able to delegate his position to another person at the Supplier but must inform the Buyer before proceeding with**

**the delegation and it will be delegated person's responsibility to fulfil the Contract Manager's responsibilities and obligations;**

**3.1.3** **able to cancel any delegation and recommence the position himself; and**

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

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

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

## 4. Role of the Operational Board

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

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

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

4.4 **Each Party shall ensure that its board members shall make all reasonable efforts to attend board meetings at which that board member's attendance is required. If any board member is not able to attend a board meeting, that person shall use all reasonable endeavours to ensure that a delegate attends the Operational Board meeting in his/her place (wherever possible) and that the delegate is properly briefed and prepared and that he/she is debriefed by such delegate after the board meeting.**

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

**5. Contract Risk Management**

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

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

**5.2.1 the identification and management of risks;**

5.2.2 the identification and management of issues; and

5.2.3 monitoring and controlling project plans.

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

5.4 The Supplier will maintain a risk register of the risks relating to the Call Off Contract which the Buyer's and the Supplier have identified.

# Annex: Contract Boards

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

TBC

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

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

Department for Energy Security & Net Zero

Invitation To Tender For:

Records Management for Coal Liabilities Unit

ITT UNDER FRAMEWORK **-** Records Information Management, Digital Solutions and Associated Services - RM6175 - Lot 5: Combined Digital Workflow, Cloud Based Hosting and Records Information Management

Tender Reference Number: prj_1489

Deadline for Invitation To Tender responses:
**13:00 2nd February 2024**

Your organisation is invited to tender for the provision of Records Management for the Coal Liabilities Unit to the Department for Energy Security & Net Zero, DESNZ ("the Department").

This tender constitutes a mini-competition under the **Crown Commercial Services (CCS) Framework Records Information Management, Digital Solutions and Associated Services - RM6175 Lot 5**

Enclosed are the following documents:

- This Invitation to Tender Letter;
- Document 1 - Instructions and information on tendering procedures;
- Document 2 - The Specification;
- Document 3 - Evaluation criteria and scoring methodology
- Document 4 - Proposed Contract Terms and Conditions
- Document 5 - Declarations: Statement of Non Collusion and Form of Tender
- Annex 1 – Market Engagement Pack (attached as separate document)

Please read the instructions on the tendering procedures carefully since failure to

comply with them may invalidate your tender which must be submitted through the DESNZ Jaggaer

web portal by the tender deadline.

You can register on the Jaggaer system via this link - https://beisgroup.ukp.app.jaggaer.com/.
Tenders for this procurement will only be accepted if submitted via the Jaggaer system.

Please acknowledge receipt of this letter by emailing confirmation of receipt of documentation to

If your organisation does not wish to submit a tender please send your reasons (although you are under no obligation to do so) to by email to the same address.

The enclosed Document 1 contains instructions for providing you with further information or clarification of the service requirement.

I look forward to receiving your response.

Yours sincerely,

[redacted]

Senior Commercial Officer

Department for Energy Security & Net Zero

**DOCUMENT 1**

**INSTRUCTIONS AND INFORMATION ON TENDERING PROCEDURES**

**ABOUT THESE INSTRUCTIONS**

1. These instructions are designed to ensure that all tenders are given equal and fair consideration. It is important, therefore, that you provide all the information asked for in the format and order specified. Please contact us via the Jaggaer Portal if you have any doubt as to what is required or will have difficulty in providing the information requested. The Department will circulate to all tenderers the content of any queries raised and the answers given if it is felt clarification would be of benefit to all tenderers

2. Please note that references to the "Department" throughout these documents mean The Secretary of State for the Department for Energy Security & Net Zero, acting through his/her representatives in the Department.

**TIMETABLE AND ADMINISTRATION ARRANGEMENTS**

**0. Timetable**

This is a summary of the timetable that applies to this procurement. The Department reserves the right to alter this timetable.

| **Event** | **Date and Time** |
|---|---|
| ITT issued | Monday 8th January 2024 |

| | |
|---|---|
| Ten Day Standstill Period | Tuesday 20th February 2024 |
| *3-month handover period with current supplier (pre contract handover) | Friday 1st March 2024 |
| Estimated Contract start date | Saturday 1st of June 2024 |
| *End of 3-month handover period with current supplier (post contract start) | Sunday 1st of September 2024 |



| | |
|---|---|
| Deadline for receipt of queries about | Wednesday 17th January 2024, **13:00** |
| Response circulated to queries | Wednesday 24th January 2024 |
| Deadline for receipt of tenders | Friday 2nd February 2024 **13:00** |
| Evaluation of submitted | Monday 5th February - Friday 16th February 2024 |
| Selection of Preferred Supplier and | Monday 19th February 2024 |

*There will be a 6-month handover period in total. 3 months pre-contract handover and 3 months post contract start date.

**0. Tender Clarification**

We may need to clarify details of your tender. This will be undertaken via the Jaggaer portal.

**1. Conditions Applying to this Tender**

The contract will end June 2028 unless terminated or extended by the Department in accordance with the terms of the contract.

**2. Incomplete Tender**

Tenders may be rejected if the information asked for is not given at the time of tendering.

**3. Returning Tenders**

Suppliers are required to submit their proposals via our Jaggaer portal. Tenders are to be returned no later than **13:00 Friday 2nd February 2024.**

**4. Receipt of Tenders**

Tenders will be received up to the time and date stated. Those received before that date and time will be retained unopened until then. Please ensure that your tender is delivered not later than the appointed time on the appointed date. The Department does not undertake to consider tenders received after that time.

**5. Acceptance of Tenders**

By issuing this invitation the Department is not bound in any way and does not have to accept the lowest or any tender and reserves the right to accept a portion of any tender unless the tenderer expressly stipulates otherwise in their tender.

**6. Period for which Tenders shall Remain Valid**

The Department requires tenders to remain valid for a period specified of 60 days from tender close date.

**7. Amendments to the Tender Documents by the Department**

11.1 The Department reserves the right to amend the enclosed tender documents at any time prior to the deadline for receipt of tenders. Where amendments are significant, the Department may at its discretion extend the deadline for receipt of tenders.

11.2 The Department reserves the right to discontinue this tendering process at any time and not to award a contract.

**8. Inducements**

Offering an inducement of any kind in relation to obtaining this or any other contract with the Department will disqualify your tender from being considered and may constitute a criminal offence.

**3. Collusion**

Please note that Document 5 contains a "Statement of non collusion"; any breach of the undertakings covered under items 1 - 3 inclusive will invalidate your tender.

**4. Costs and Expenses**

You will not be entitled to claim from the Department any costs or expenses that you may incur in preparing your tender whether or not your tender is successful.

**15. Debriefing**

Following the award of Contract, a written debrief will be provided on

request. **16. Tender Documents**

Your tender response should, unless otherwise agreed, be word-processed using a font of no less than 12 point and should be written in English and be no more than requested number of pages long. All pages should be consecutively numbered and the total number of pages must be indicated on each page.

**3. Confidentiality**

**Please note the following requirements, you must not:**

- Tell anyone else what your tender price is or will be, before the time limit for delivery of tenders.
- Try to obtain any information about anyone else's tender or proposed tender before the time limit for delivery of tenders.
- Make any arrangements with another organisation about whether or not they should tender, or about their or your tender price.
- Share the attached Annex with anyone outside your organisation. Failure to

comply with these conditions may disqualify your tender.

**18. Freedom of Information and Transparency**

18.1 The Freedom of Information Act 2000 ("FOIA") and the Environmental Information Regulations 2004 ("EIR") apply to the Department. You should be aware of the Department's obligations and responsibilities under FOIA or EIR to disclose, on written request, recorded information held by the Department. Information provided in connection with this procurement exercise, or with any contract that may be awarded as a result of this exercise, may therefore have to be disclosed by the Department in response to such a request, unless the Department decides that one of the statutory exemptions under the FOIA or the exceptions in the EIR applies. If you wish to designate information supplied as part of this response as confidential, of if you believe that its disclosure would be prejudicial to any person's commercial interests, you must provide clear and specific detail as to the precise information involved and explain (in broad terms) what harm may result from disclosure if a request is received, and the time period applicable to that sensitivity. Such designation alone may not prevent disclosure if in the Department's reasonable opinion publication is required by applicable legislation or Government policy or where disclosure is required by the Information Commissioner or the First-tier Tribunal (Information Rights).

18.2 Additionally, the Government's transparency agenda requires that tender documents (including ITTs such as this) are published on a designated, publicly searchable web site. The same applies to other tender documents issued by the Department (including the original advertisement and the pre-qualification questionnaire (if used)), and any contract

entered into by the Department with its preferred supplier once the procurement is complete. By submitting a tender you agree that your participation in this procurement may be made public. The answers you give in this response will not be published on the transparency web site (but may fall to be disclosed under FOIA or EIR (see above)). Where tender documents issued by the Department or contracts with its suppliers fall to be disclosed the Department will redact them as it thinks necessary, having regard (inter alia) to the exemptions/exceptions in the FOIA or EIR.

5

**19. Prompt Payment Policy**

19.1 The Department aims to pay all correctly submitted invoices as soon as possible with a target of 10 days from the date of receipt and within 30 days at the latest in line with standard terms and conditions of contract.

19.2 A correct invoice is one that includes:

- the date, supplier name, contact details and bank details;
- the agreed charge;
- confirmation that the goods / services detailed have been fully performed;
- the valid purchase order provided by the Department;
- delivery to the nominated address.

19.3 Any correctly submitted invoices that are not paid within 30 days may be subject to the provisions of the Late Payment of Commercial Debt (Interest) Act 1998.

**Please note the framework terms and conditions will be applied to this contract.**

**DOCUMENT 2**

**THE SPECIFICATION**

**DPF4**

**SPECIFICATION**

**Title:**

**Tender Reference Number:prj_1489**

Call-Off Ref:

Crown Copyright 2020

8

Framework Ref: RM6175

Project Versi

# Introduction and summary of requirements

The Government manages the records of the former British Coal Corporation. This is a combination of business documents and personal data which includes a significant number of historic occupational health claims files. In part, this is to enable us to respond to disease/illness personal injury claims arising from working for the Corporation pre-privatisation in 1994. We also have a duty to ensure that the information is kept safe and is managed securely.

We require a service that enables:

- secure storage of over 2.8m physical records and 47m digital records
- the ability to retrieve these promptly and to provide them to the public and the Department's contractors as appropriate
- scanning of physical records for onward processing
- preparation and transfer of records to The National Archives
- disposal of records no longer required
- the hosting of a digital platform that allows contractors to access records
- the facility to search documents in terms of categories, e.g various types of colliery minutes and key work searches.

The successful bidder will need to work closely with the Department's external solicitors to facilitate swift access to records as and when required.

### Cost requirement

A direct point of contact must be identified from the outset to manage and respond to all financial related queries. A clear and consistent pricing list will be used for the entire length of the contract and must be agreed before work begins.

# Background to the records

In 1998, the then Department of Trade and Industry ("DTI"), now the Department for Energy, Security and Net Zero ("DESNZ"), assumed responsibility for the records and archives belonging to the former British Coal Corporation ("BCC").

Whilst those records relating to mining activities were allocated to the Coal Authority, large volumes of records relating to details of employees remain the responsibility of the Coal Liabilities Unit (“CLU”) within DESNZ, along with a number of other coal mining related records.

In addition, a considerable volume of documents has also been generated by, and on behalf of, CLU in connection with administering the resolution of compensation claims by former mine workers. The records are wide-ranging in terms of their format and origin. Some of these records will need to be retained for a considerable number of years in line with legal obligations (e.g. for medical records).

CLU is committed to managing all records efficiently, making them accessible when needed, protecting and storing them securely and disposing of them safely at the appropriate time.

Efficient long-term storage of these records and the need for future access to this information for ongoing or potential litigation requires a flexible records management

service. Such a service also needs to deliver solutions for maintaining access to the data and outputs that exist on legacy databases, which are held by the incumbent records management supplier.

## Overall Contract Objectives

DESNZ is responsible for ensuring that all contracts deliver Value for Money ("VFM") to the public purse and has set out below its main objectives. These align with DESNZ's overall strategic objective to manage energy related liabilities efficiently.

The Service Provider (SP) must proactively meet the following objectives, which are critical to the success of the contract and it should clearly articulate how it intends to do so.

1. The SP must have a thorough understanding of all of the core services required and the ability to provide the infrastructure to deliver the core services as described in the Specification.
2. The SP must be able to manage a large scale contract involving both electronic and hard copy records.
3. The SP must be able to provide a flexible service and ramp up/down the service if the volumes increase/decrease significantly.
4. The SP must provide safe and cost effective long term storage.
5. The SP must protect all Personal Data held on behalf of the CLU.
6. The SP must provide a service which delivers VFM and ongoing performance and cost improvements.
7. The SP must work in partnership with the CLU's staff and other service providers and stakeholders who use the records.

## Records held by the CLU

Former British Coal Records

In 1998, the DTI assumed responsibility for the records and archives belonging to the former BCC which were distributed between the Coal Authority and the CLU. The

Coal Authority assumed responsibility for records relating to mining activities. These records are stored under a separate arrangement and are not being tendered for within this Specification. The CLU within DESNZ maintains responsibility for records (and associated records), including those which affect former employees of the former BCC including personnel records, training records, earning records and Health & Safety minutes. These records are held in hard copy and electronic format and require ongoing storage and servicing until a destruction regime is implemented in the future.

Personal Injury Claim Records

In addition to BCC records, new records have been generated relating to coal health claim schemes and individual personal injury claims which form part of this Specification. In January 1998, the High Court found the BCC negligent in respect of

lung disease caused by coal dust, known as Chronic Obstructive Pulmonary Disease (“COPD”). In July 1998, the Court of Appeal confirmed an earlier High Court decision of negligence in respect of hand injuries caused as a result of using vibrating equipment, known as Vibration White Finger (“VWF”).

CLU, in negotiation with the Claimants Solicitors’ Groups (“CSG”), who represent the interests of claimants, and subject to the approval of the High Court, introduced two schemes, one for COPD and one for VWF, to compensate miners (or their widow/estate). Potential claimants made applications for compensation via their legal representatives. The schemes are now closed and all claims processed. There have been circa 590,000 claimants for COPD and circa 170,000 for VWF.

In addition to the main schemes, there is a significant group of compensation claims known as (“Miscellaneous Diseases”) which incorporate all claims for conditions other than those covered by the main COPD and VWF schemes. Generally, these claims are handled on a common law basis and dealt with on their own merits. The largest category of these claims is for industrial deafness or Noise Induced Hearing Loss (“NIHL”). Other claim types include asbestos-related diseases, cancer, nitroglycerine headaches, occupational asthma, upper limb disorder and accidents. CLU’s forecast indicates that litigation for Miscellaneous Disease claims will continue until around 2065. Therefore, there is an ongoing servicing requirement in line with this relatively small number of claims.

The SP must be able to provide record management services in line with this Specification to support the remaining claims and ongoing servicing requirements of the Miscellaneous Diseases.

## Generic Requirements

The SP must manage and control the requirements of the records management services efficiently and effectively. CLU needs a contractor who proactively manages the business efficiently and significantly contributes to strategic and operational matters to ensure the provision of a quality service which is reliable, consistent and delivers VFM.

The SP must allocate and maintain adequate and appropriate resources for all aspects of the contract, ensuring compliance with all requirements specified in the Invitation to Tender (“ITT”) documents, legislation and professional standards.

Sufficient staff of the correct grade, competency and level of experience must be utilised to ensure that the SP can deliver a quality service.

A robust training and development programme is a key requirement and operational staff, in particular, must be comprehensively trained and made aware of their roles and responsibilities and the SP must demonstrate how this will be maintained throughout the life of the contract.

## Service Requirements for Management Information and reporting

The SP must meet all of the objectives as set out above.

The SP must have information tools to accurately and efficiently deliver MI within the agreed timescales set out by CLU. The minimum MI requirements are indicated below. The type and frequency of the MI will be agreed during the transition period. It will be reviewed at least every six months to ensure it continues to meet CLU's requirements.

The SP must accept that MI reporting may change from time to time at the discretion of CLU and that all such reasonable changes will be implemented at no additional charge by the SP.

Monthly Reporting

The SP must provide a monthly MI report within ten working days from the end of the previous month by e-mail to nominated CLU staff. The report will contain, as a minimum:

- Monthly activity data including storage volume;
- searches;
- regulatory access requests;
- records shared;
- destruction.
- Trend analysis
- performance against Service Level Agreements ("SLAs")
- number and nature of complaints and resolution actions;
  - risk and issues log
  - details on any non-compliance against SLAs and remedial actions taken to ensure non-compliance does not reoccur.

Ad-Hoc MI

The SP must be able to provide MI on request. Examples of this could be:

- to respond to a Parliamentary Question ("PQ") from a Member of Parliament;
- to respond to external scrutiny bodies such as the NAO;
- to update Ministers and senior officials; and
- to provide information for internal audit.

These requests may be recorded as ‘Urgent’ requests and should be responded to within the relevant SLA.

The SP must provide to CLU all information and assistance necessary (and in such format as may be specified by CLU) to enable CLU to monitor the provision of the services by the SP. For the avoidance of doubt, the SP will not charge for any additional MI reasonably requested by CLU.

Annual MI

In addition to the requirements above, at the commencement of the contract, the SP must supply to CLU and update at least once every year, the following documents:

- a ‘services manual’ produced by the SP detailing all aspects of the provision of the services by the SP, including inter alia, descriptions of procedures and

processes, organisation and management teams, staff, audit/open book procedures, security (the “Service Manual”);

- annual compliance statement from the SP’s account manager confirming robust data handling;
- The Disaster Recovery Plan (“DRP”) in accordance with Contract Terms and Conditions (Disaster Recovery and Disruption).

Monthly Meetings

The SP must attend monthly contract meetings. These will be to discuss the progress of the contract and current issues affecting MI. Contract and Operational Managers should attend. There may be a requirement to conduct further ad-hoc meetings in addition to the meetings set out below. The SP must attend and support any such meetings which are identified. For the avoidance of doubt, any such request will not represent a change of service and shall be at no extra charge to CLU.

# Communication and Stakeholder Management

The purpose of this section is to specify what is required of the SP in relation to communication and stakeholder management.

Background to communication and stakeholder management

The work of CLU remains high profile in parliament and in former coal mining areas. We deal with sensitive issues and there are a significant number of stakeholders involved. Clear and consistent communication is essential to ensuring that all stakeholders remain informed where necessary. Equally, the litigation context of the work means that relevant protocols on access arrangements need to be followed as directed by CLU.

CLU handles a range of information requests including PQ’s, ministerial

correspondence, requests under the Freedom of Information Act 2000 (“FOI”) and enquiries from claimants and other stakeholders. Enquiries from journalists are handled by the DESNZ Press Office. The SP must direct all enquiries from journalists to CLU.

CLU has statutory and self imposed deadlines to meet when responding to the various types of requests. For example, requests under the Freedom of Information Act 2000 require a response within 20 working days. When CLU are responding to parliamentary questions, CLU have to provide a response within 48 hours, therefore the SP would be required to respond to CLU within 24 hours. In order for CLU to meet deadlines, the SP must produce the information promptly, and in accordance with the SLAs, to enable compliance.

Key Stakeholders

The SP is required to build effective working relationships with CLU stakeholders, as guided by CLU, in order to assist CLU in continuing to maintain a collaborative working environment. These include:

CLU – the SP will need to respond to requests from the CLU.

Other Government Departments – require ongoing access to the records including, for example, requests from the Department for Work and Pensions ("DWP"), for use in benefit schemes including Industrial Injuries Disablement Benefit.

Claims Handlers (currently NCS) – will require ongoing access to record packs and medical data to assist in the assessment of claims for compensation.

NCFO (currently Capita) – will require storage of new and existing records and retrieval.

CLU's External Legal Advisers (currently CMS) – will require ongoing access to records to support their work in assessing the Department's coal health liabilities. The National Archive ("TNA") – will require access to documents categorised as being of national importance and have clear guidelines to be followed in interaction with them.

Objectives for communication and stakeholder management

- To ensure that CLU receives timely, full and accurate information as requested in order to respond to enquiries.
- To support CLU and other third parties in producing timely communications as required.
- To work effectively with NCS, CMS and other third parties to progress and settle claims.
- To build effective working relationships with stakeholders as directed by CLU

Managing Complaints & Disputes

The purpose of this section is to specify what is required of the SP in relation to the management of complaints and disputes.

Background to managing complaints and disputes

A complaint is defined as an expression of dissatisfaction in relation to the services provided by the SP not just to DESNZ but to any of the stakeholders. Complaints can be received from different parties for a variety of reasons. Such reasons could be because of poor service, time delays, inaccurate information, misunderstandings or any other such reason which means any party was unhappy with the service

provided. The sensitive nature of the services means that all complaints should be handled promptly, professionally and in a timely manner.

Objectives for managing complaints

- To put in place processes to manage and rectify complaints.
- To record, report and escalate to CLU any complaint received from any party (see section 6 on MI).
- To assess the MI regarding complaints and complete root cause analysis to determine any systemic issues, the results of which should be shared with CLU.
- To ensure all complaints are handled effectively.

Service Requirements for managing complaints only

1. The SP must meet all the objectives set out above.

2. If the SP receives a complaint directly, they must:

- Record and track the complaint through to resolution with all associated actions.
- Inform CLU of the complaint within five working days and provide a copy of the complaint correspondence.
- Provide a monthly report of all complaints as part of the monthly management reporting (see section 6 on MI).

3. The SP must respond in writing to the complainant within five working days from receipt of the complaint.
4. The SP must use all reasonable endeavours to resolve the complaint.
5. Where complaints are not resolved to the satisfaction of the complainant, the SP must report these to CLU. The levels below show the stages through which the handling of a complaint must be escalated.
6. The SP must assess the complaints received to determine whether there are any systemic reasons for them. The SP must report to CLU on their proposed approach to resolution and put in place rectification measures if there are found to be systemic reasons, within a timescale agreed by CLU.

Level 0 - An expression of dissatisfaction is raised and resolved by the SP.

Level 1 - The expression of dissatisfaction cannot be resolved by the SP and requires intervention from the CLU Contract Manager.

Level 2 - The expression of dissatisfaction requiring intervention from the Contract Director.

Level 3 - Serious complaints requiring intervention from the CLU Director.

CLU expects disputes to be minimal and will expect that operational difficulties will be handled professionally in accordance with good programme and service management protocols. However, if disputes do occur, they will be handled in line with the Terms and Conditions of the contract.

# Background to audit

As part of the CLU's approach to robust contract management, audits are periodically conducted across all SPs to ensure adequate controls are in place. A risk-based

approach is adopted to determine which areas to audit. There are four main types of audit activity which will be invoked from time to time:

(1) DESNZ Internal Audit ("IA") Programme

The Government Internal Audit Agency (GIAA) provides internal audit services to DESNZ.

(2) Compliance Audit

Regular reviews are conducted to provide assurance on invoice accuracy and performance against SLAs.

(3) Other Audit Related Activity

CLU reserves the option to commission audit reviews of the SP on an ad hoc basis from our advisers, such as its external legal firm, CMS. Examples of ad hoc reviews on records management could be on an information audit of the top-level record sets held by the CLU suppliers and an activity related audit to review record collections with the aim of retention, destruction or consolidation.

(4) SP IA Programme

CLU expects its key SPs to have their own IA teams who will conduct reviews on the adequacy of controls and other relevant issues. The future programme of such audit

activity in relation to the services must be shared with CLU together with the findings of these audits.

Objectives for audit

The main objective of IA work (both CLU and SP's IA) is to ensure that adequate controls are in place to prevent disruption to the services, especially in the higher risk areas of handling of Personal Data and data security.

Service Requirements for audit

1. The SP must meet all of the objectives as set out above.
2. The SP must proactively support and co-operate with all audit activity which should include the effective use of the SP's own IA team.
3. The SP must have an appropriate management structure in place to ensure that sufficient resources are available at a senior level to oversee the audit process as well as to respond to requests and queries from either of the audit teams.
4. CLU's audit team must have complete right of access to all related information, relevant locations, IT systems, documentation and personnel in order to undertake any audits as required by CLU.
5. CLU, its agents and professional advisers shall have the right to conduct on and off site audits of the SP and any subcontractors pricing as identified in the pricing schedule and any aspects thereto.
6. The data and information provided to the auditors must be accurate, transparent and consistent. For the avoidance of doubt, CLU will not pay for the collation and provision of data to enable audits to proceed.
7. Information requests, queries and responses must be provided in a timely manner.
8. Recommendations from the audits must be implemented within agreed timescales or alternative arrangements agreed with CLU.
9. The SP must report to CLU on its own audit outcomes insofar as it relates to the provision of services under this contract.

Future Audits

Compliance audits for invoices and SLAs will be conducted on a regular basis. The focus of future internal audits will be determined by the risks around key processes, but are likely to include:

- A post SP transition audit to ensure that the objectives of the transition process have been achieved and that live services can commence at 1 June 2024 (see section - Transition).
- Data handling and security, business continuity/disaster recovery and compliance with the Data Protection Act (“DPA”), UK General Data Protection Regulation (“UK GDPR”), FOI and Environmental Information Regulations 2004 (“EIR”) and associated regulations and legislation.
- Compliance by the SP with the CLU Records Management Policy.

## Risk Management

The purpose of this section is to specify what is required of the SP in relation to risk management.

Objectives for risk management

- To have an effective risk management process in place.

- To work in a constructive way with CLU to identify and mitigate risks.
- To have suitable resources in place to oversee and monitor potential risks.
- To have a strong risk management culture and framework in place throughout the entirety of the contract.

Service Requirements for risk management

The SP must meet all of the objectives as set out above.

The SP must maintain a record of risks and issues ("Risk Log") which could affect any part of the services. This Risk Log must be shared with CLU on a monthly basis as part of the contract meeting (see section 6 on MI). The format will be agreed by the SP and CLU before it is implemented.

The SP must raise any new risk concerns with CLU and work with CLU to confirm the actions being taken to mitigate these.

The SP must have robust processes and procedures in place to identify and analyse risks and demonstrate the steps taken to mitigate the risk.

# Financial Management

The purpose of this section is to specify what is required of the SP in relation to financial management.

Objectives for financial management

- To have clear and auditable monthly invoicing systems in place.
- To ensure it has robust financial management procedures and systems in place which will withstand external scrutiny.
- To have clear audit trails for all financial transactions.
- To support the CLU in producing robust financial information and reports.
- To support any scrutiny from external bodies such as NAO or HM Treasury.
- To ensure financial controls are in place for any sub-contractors where used.
- Overall, be able to demonstrate VFM.

Service requirements for financial management

The SP must meet all of the objectives above.

Financial Controls

The SP must have strong financial controls in place to ensure that it can record and report accurately to CLU and other third parties.

Monthly Invoices

The SP must submit accurate invoices on a monthly basis for processing and payment.

The SP must issue invoices no later than 10 days following the end of the month. The SP must ensure invoices are submitted together with all supporting documentation for the billed services. This documentation should include, inter alia, activity details, volumes, unit costs and explain any ad-hoc charges. CLU will not be liable for the payment of invoices that are not submitted with all relevant and supporting documentation.

Ad-hoc financial information requests

The SP must be able to produce ad hoc financial reports from time to time as required by CLU. These reports may be used to support internal CLU meetings or externally with parties such as HM Treasury and the NAO.

Audits/External Scrutiny

The SP must allow CLU, or its nominated advisers, to examine its financial controls as and when required. The SP must provide suitable resource to support this process.

## Business Continuity and Disaster Recovery

The purpose of this section is to specify what is required of the SP in relation to Business Continuity and Disaster Recovery.

Background to business continuity and disaster recovery

It is essential that if there is an incident, the services being provided are restored and recovered to an acceptable level over an agreed timescale. CLU expects a business to be able to continue with the services it provides in event of a disaster occurring. The SP must ensure they can continue the service in the event of a disaster. It is important that, in the event of any disruption to the records management services, the services become fully operational as soon as is logistically possible. The SP must have business continuity and disaster recovery procedures in place. More information regarding business continuity and disaster recovery can be found in the Terms and Conditions.

Service Requirements for business continuity and disaster recovery

The SP must have in place procedures to recover and restore partially or completely interrupted critical function(s) within a predetermined time after a disaster or extended disruption.

The SP must have in place procedures to handle incidents which might include building fires, floods, a prolonged loss of power and IT downtime and other events determined from time to time.

Business Continuity and Disaster Recovery Plan ("DRP")

As part of the business continuity planning, the SP must establish prior to execution of the contract, and must maintain at all times, a DRP to include preventative and remedial steps to be taken in the event of interruption to the services or business processes, to ensure continuity of the service or to recover data and other IPR. The DRP must be approved by CLU and the SP must, in the event of interruption of the services, act in accordance with the same. The cost of such act will not be charged to CLU. The plan must contain:

- the schedule of all data which is the subject of the DRP;
- the identification of all the threats facing core records management services including, inter alia, an assessment of physical security, a vulnerability analysis, the impact of loss and the implementation of safeguards to counter critical risks;
- fully documented procedures to invoke when the DRP is enacted (when and how a disaster shall be determined to have arisen);

- contracts, insurance, invocation process and the actual recovery plan and a telephone list of both CLU and the SP personnel external contacts. The DRP must include documented procedures covering all actions by the nominated personnel and will be reviewed and tested at least annually to ensure the procedures are working as designed and are robust. The outcomes of the annual test must be reported to CLU at the next Monthly Contract Review meeting;
- criteria for the annual test and how this will be reported. CLU must be given the right to observe the annual test;
- business impact analysis, identifying the critical applications, setting up the recovery teams, defining the scope and objectives of recovery and putting in place a training mechanism to increase the awareness of all employees of their role, detailed documented procedures for recovery including the identification of a location for backup media, operational procedures, scripts for job completion and other material required for recovery; and
- the telecommunications provisions to connect to recovery sites if no permanent connection exists.

The SP must update the DRP in response to the findings of the Disaster Recovery Exercise referred to above and at other times as dictated by application or environment changes.

Recovery of Applications

The SP must recover the applications to a consistent point at the end of Normal Service Hours before the disaster occurred within the timescale for recovery as defined in the DRP for the applications.

Annual Tests

The SP must conduct the Disaster Recovery Exercise. The first annual test must take place no later than December 2024 with a full report on the outcome made available to CLU by the end of January 2025. The test criteria must be specified in the DRP.

Invoking the DRP

The SP must inform CLU immediately of any necessity to invoke the DRP.

Use of a third party

If the DRP involves the SP entering into any agreement with a disaster recovery service provider, such an agreement shall be subject to CLU's prior written approval. Any such agreement or approval must not prejudice or affect the liabilities of the SP under or in connection with the contract and the SP should be fully liable for the acts and/or omissions of any recovery service provider acting on its behalf. If the SP plans to make use of a third party(ies) as part of the DRP, this must be made clear in the response to this ITT.

Background to storage

CLU has both hard copy and electronic records. Hard copy records are currently managed by the incumbent in a record storage facility on the outskirts of Stafford. This is a shared facility, owned and used by the incumbent SP to store documents for a variety of organisations. At July 2023, there were 20,327 linear metres of CLU records stored there.

There is approximately 12,500 Gigabytes (GB) of electronic records stored and managed by the incumbent SP.

Records are a combination of ‘record packs’ created for all known former BCC employees. These were originally collated in hard copy and subsequently scanned to create electronic record packs, with both versions still in storage. Each record pack contains (where available) personnel, training, common law and earnings records for a former employee. There are further electronic record packs for anyone who has ever made a claim for compensation.

The majority of the documentation relating to claims already exists and there are not expected to be major additions to the volume of records currently being managed. However, any new litigation against CLU would be expected to generate new documents.

It is possible that the original hard copy records could be required, and therefore, retrieval of them from storage will be in scope. Currently, there is little activity relating to hard copy records. There are two main reasons why these records must be carefully stored. Firstly, original paper documentation may be required as part of any current or future litigation. Secondly, all of the documentation comprises Government-owned historical records.

The SP has a responsibility to care for and maintain their integrity unless otherwise instructed by the CLU. The majority of electronic records are scanned images of paper record packs. Other electronic records contain former British Coal employee information, earnings records and medical records. As with hard copy records, the integrity of all electronic record packs must be maintained as they are integral to current and any future compensation claims.

CLU’s claims handlers expect the SP to provide electronic record packs in response to all data access requests within strict deadlines, unless otherwise advised. Other electronic records may also be required as part of compensation claims or other requests. As a result, the SP must have the safekeeping of CLU’s records as one of its highest priorities.

Objectives for storage

- To store and keep secure all hard copy and electronic data owned by CLU under the scope of this contract to ensure and that the integrity of all CLU data is fully maintained and not compromised. Records should be stored in the most economic and effective way possible.
- To provide resources and facilities capable of processing and storing fluctuating volumes of documentation relating to the former BCC and the CHCS over the lifetime of the contract managed by the SP. This includes the addition and removal of records over the life of the contract.
- All records regardless of format should be accessible and readable for as long as CLU requires them.
- Electronic records should be securely managed within a compliant environment to maintain their integrity and authenticity. Migration to IT infrastructure will be necessary so that electronic records remain accessible and readable.

Service Requirements for storage

20

Storage

The SP must meet all of the objectives set out above.

The SP must ensure that it is capable of receiving, storing and safeguarding any additional documentation relating to BCC or current and potential claims for as long as CLU requires.

The SP must maintain up to date information on all records owned by CLU under its care throughout the life of the contract, and provide reports on this to CLU in accordance with the requirements detailed in the MI section.

Security for storage and storage facilities

The SP must provide secure locations for the storage of all hard copy paper records and all hardware (e.g. servers, disks, tapes or removable media) holding or processing electronic records in accordance with BS7799, ISO 27002 and ISO 27001, or equivalent.

The SP must ensure all records carry the appropriate protective markings in line with Government standards.

The SP must complete periodic reviews of the security for storage and storage facilities to take account of any changes to physical security for the secure locations or an increased threat to the Personal Data held.

The SP must keep all servers and other hardware (both primary and backup) in dedicated locked facilities within secure storage locations.

The SP must ensure that up-to-date backups of all electronic data are taken. Full backups of all electronic information must be taken once a week at a secure location away from where the data is stored. The SP must also take incremental backups on a daily basis. The SP must complete at least 1 backup verification exercise biannually.

The SP must have processes and procedures in place that allow backed up data to be restored to the live environment if required within 24 hours of a request for restoration being received.

The SP must ensure that all security countermeasures required to protect the live servers are equally implemented at the location(s) of backup servers, tapes and disks.

The SP must provide 24 hour security monitoring, including adequate CCTV to monitor the physical environment where hard copy records, electronic records and back up records are stored.

The SP must provide access control systems at all storage locations to ensure only authorised personnel can access the storage locations and prevent unauthorised access. Personnel must be properly trained and appropriate checks made as part of their recruitment and selection.

The SP must seek CLU's approval prior to access being granted to any individual:

- The SP must only grant access to a visitor accompanying an authorised person if the visitor provides photographic ID in the form of a passport or driving licence to demonstrate their identity.
- The SP must ensure that details of all visitors and who they are accompanying are recorded, showing the visitor's name, the visitor's company name, contact number, the name of the authorised person they are accompanying, the purpose of the visit, the date of the visit, the time of entry to the storage location and time of departure.
- The SP must provide CLU with a record of visitors, requesting access to CLU hard copy and electronic records, to any storage location on receipt of a written request from CLU and at least annually.
- The SP must maintain a record of all personnel with the ability to access the secure locations. The SP must provide this list at any time on receipt of a written request from CLU and at least annually.

The SP must maintain a written record of all requests made for access to the dedicated locked facilities used to store servers, hardware and electronic media, with access granted only to necessary appropriately checked and, technical personnel. The SP must ensure all keys to these dedicated locked facilities must be signed-out by the requester, and signed back in upon their return. A record of this must be kept and made available for inspection by CLU on receipt of a written request.

The SP must be able to provide an audit trail of access to the records as described above in line with retention periods set out by CLU.

Environmental Controls

The SP must ensure that storage locations are designed and located to minimise the risk of damage to records, including from fire, flooding and other water damage, vermin and /or pests, temperatures and/or humidity, breaks in the power supply or power surges.

# Requests for Information

Background

While the SP's primary responsibility is to keep safe all records under its management, it must also be able to process access requests from a variety of sources.

The SP needs to service all requests from all sources in line with the requirements set out below, however there are specific regulatory requirements which the SP must be aware of and handle those requests in line with specific requirements.

When processing data, CLU is required to comply with a range of regulatory obligations, in particular the DPA, the FOI Act and the EIR, collectively known as Regulatory Access Requests ("RARs"). Should CLU fail to comply with these regulations, it risks regulatory sanctions and enforcement action from the Information Commissioner's Office ("the ICO"). CLU's current processes for managing RARs are detailed below. The processes do not apply to any other requests received by the SP.

Objectives for requests for information

- To ensure access requests of any type are processed accurately, enabling documents requested to be retrieved within the timescales contained in the SLAs.
- To comply with timeline requirements set out by CLU.
- To ensure those staff processing RARs are appropriately trained to correctly identify RARs.
- To support CLU in its compliance with RARs.
- To provide assistance to CLU in meeting all legal, regulatory and formal requests from inter alia, Law Enforcement Agencies, Government Departments and Regulatory Bodies.

Current process for requests

The incumbent SP currently runs a service, on behalf of CLU, which handles requests for information and records. These requests can come from a variety of sources which include, but are not limited to, CLU, solicitors, The Coal Authority, the National Concessionary Fuel Office (NCFO), the Department of Work and Pensions (DWP) and members of the public.

These requests for information are currently only accepted in written form, either by letter or email. If a phone request is received, a form is sent by the SP to the requester, and the request processed upon its subsequent return to the SP. In all cases, these requests for information can only be processed and copies of records provided to the requester if processing of the request is permitted by legislation. A request for information under one of these regulatory obligations must be processed in accordance with the requirements detailed below.

Current Process for handling RARs

RARs received are processed under three separate processes defined by CLU, depending on which one of the regulations the request falls under. In general, the SP is expected to take the lead role in DPA requests, and CLU will lead on FOI and EIR requests. RARs, once received, are sorted by specific regulation. For the avoidance of doubt, the SP will not be entitled to charge the requester a fee for the information request and subsequent issue of data.

DPA: Subject Access Requests

DPA is the main piece of UK legislation governing Personal Data protection. Section 7 of the Act provides the right of subject access, whereby individuals can request access to their own data. As the Data Controller, CLU has responsibility for fulfilling such requests in compliance with the DPA. The SP must take the lead in handling DPA requests on behalf of CLU.

The SP on behalf of CLU must comply with the subject access request within 40 calendar days of receipt, by providing the necessary information to the individual ("Data Subject") who has made the request. The 40 day time limit, begins when the

SP on behalf of CLU, has received the information required to satisfy it as to the identity of the Data Subject.

The SP must ensure that they can competently handle DPA requests in line with the legislation. It must ensure that exemptions are accurately applied and any third party personal data is redacted in the final response.

CLU must be informed of all requests and complaints within 5 workings days and also copied in on the final response from the SP to the data requester until such time as CLU determine.

Freedom of Information Act (FOI)

Under the FOI, anyone, wherever based, has the right to ask for information held by CLU. There is a duty on CLU to make information readily available to the public on request. This is separate from the duty to supply information to the applicant. There are a wide number of exemptions and conditions in the FOI which affect these duties.

There is also a “duty to advise and assist” the applicant. If CLU does not hold the information itself but is aware of where it might be obtained, then it is required to help the applicant by telling them where it can be found. In all cases, the SP must be able to support CLU in this process where the SP is processing data on its behalf.

The statutory requirement is that all requests for information must be dealt with, and the information supplied, within 20 working days of receipt of the request. This is a maximum time limit and the Information Commissioner's Office expect requests to be dealt with as soon as is practicable and that there should be no unnecessary delay. If the applicant is asked for further details in order for the information to be located, the 20 days are suspended until the day after further details are received.

If the ‘public interest test’ (that there is a general public interest in disclosure) has to be applied to a particular request, and if this is likely to take longer, the 20 days can be extended. However, the applicant must be informed of the reason for the delay and given an estimate of when the matter will be resolved.

Environmental Information Regulation (EIR)

The EIR 2004 applies to most public authorities in addition to any organisation carrying out a public administration function, or is under the control of a public authority which has environmental responsibilities. This can include private companies or public private partnerships.

Public authorities must comply with any requests within 20 working days of receiving the requests or from receiving further information, if further information is required. An extension of an additional 20 days can be made if the request is particularly complex or large.

In all cases, the SP must able to support this process where the SP is processing data on its behalf. Persistent failure to respond within the time limit will lead the ICO to consider enforcement action.

Service Requirement for requests

The SP must have a dedicated central point of contact in order to deal with all enquiries received from CLU and other third parties. The SP must ensure that the enquiry service processes are secure, while being easy for Users to understand and use.

The SP must handle all requests received in relation to CLU records and establish communication channels with the key Users of the information.

The SP must have a mechanism in place to receive enquiries via telephone, post and also have a dedicated email address. The SP must provide and make available these contact details. The SP may also choose to have a secure online service provision.

The SP must only process written enquiries through the enquiry service. This can be in the form of an email or letter or via any online service. If a request for information is received by phone, the SP must send the requester a request template by email or post to complete and return to the enquiry service or provide information on how to use any online service provision.

The SP must process information requests within the timeframes allowed by the SLAs and have the facilities to track and monitor enquiries. This is to ensure a clear audit trail.

The SP must provide information in either hard or electronic copy (or both) in response to a request processed by the enquiry service. The SP must provide hard copies of documents (e.g. photocopies) if asked for in a request processed by the enquiry service.

The SP must maintain complete records of all information requests and record activity including:

- who has requested access on behalf of whom, if applicable;
- extent and nature of access requested;
- the legal basis for the requests;
- the nature of information copied/scanned and dispatched to requester;
- time taken between the receipt of the requests and the point of dispatch; and

- confirmation of original documentation having been replaced accurately after copying/scanning.

The SP must present requests for access on forms specified and agreed by CLU from time to time. The SP must retain all such documentation for at least 6 years after the delivery of the requested services unless otherwise agreed by CLU.

The SP must have the staff and facilities to deal with requests and provide the services relating to all records during Standard Working Hours and be required to provide a retrieval service outside Standard Working Hours to meet specific deadlines; however this will be discussed and agreed in advance with the SP.

Keyholders and means of contact must be notified to CLU for each records storage location, to provide for emergency access to records outside of Standard Working Hours.

RAR requirements

The SP must ensure all RARs are fully and correctly identified, registered and processed according to CLU's current and any future guidelines.

The SP must ensure there is an appropriate infrastructure, procedural and resource framework to support CLU in discharging its regulatory responsibilities for identifying RARs and escalating complex, sensitive cases and complaints immediately to CLU.

The SP must ensure that all RARS are tracked and managed within the time frame specified by CLU.

Activities must include:

- identifying the request as a RAR and promptly notifying relevant parties of the request. All FOI and EIR requests must be notified to CLU within 48 hours of receipt and prior to any information being released;
- retrieving and providing a copy of all relevant information in its possession/ control, along with any information required to make the data intelligible;
- processing information requests made by CLU in dealing with FOI and EIR requests. Responses must be provided within 5 working days;
- co-ordinating activities with other CLU contractors where appropriate;
- ensuring information provided is correctly limited to the scope of the request;
- ensuring processes are developed and put in place for effective management of partners and/or subcontractors to facilitate the seamless management of access requests;
- ensuring staff managing RARs are skilled, trained and resourced and kept up to date with their roles and responsibilities; and
- producing monthly management information of all RARs received and processed, and submitting confirmation that all RARs are managed within the processes and procedures set out in this document. Specifically where information is not found or withheld for whatever reason should be detailed within the monthly report. This information is to be provided to CLU as part of the monthly management information report and when requested by CLU.

For DPA requests the SP must inform CLU of all requests from a Data Subject to have access to that person's Personal Data; or any complaints or requests relating to CLU's obligation under the Data Protection Legislation within 5 workings days.

The SP must copy CLU with the final response on all DPA access requests until such time as notified by CLU.

## Searching, indexing and filing

Background to searching, indexing and filing

In most cases, the SP will be provided with information such as NI number, name, date of birth, colliery in order to search for hard copy or electronic records. The function of searching should provide either a positive result in which either a hard copy record can be retrieved or an electronic record can be simply uploaded.

There are also exercises when the SP will be required to search using “key words”. The SP will be provided with a number of key words in order to identify records which may contain these words. The SP will then provide a printout in a suitable format with the outcome of the search and a list of successful title of records containing the key words. This will be passed to the requester, who will advise whether they require the

SP to retrieve the records or provide a refined list of key words for the SP to search against. This process can be iterative.

Most of the records managed by the SP are static. There is currently very little movement of hard copy records and the volume of cataloguing and filing activity is very limited. However, there remains the possibility of future litigation, which could require the SP to take additional new records under its management and greatly increase the search frequency. The exact volume of future filing requirements is difficult to predict, but the SP must have processes in place to correctly index and file new documentation and/or remove existing entries from the index. In future, CLU would envisage any new documentation coming under the SP's management to be indexed and filed in a manner to allow its subsequent retrieval if required. Although the indexing of some existing records may be of a variable standard, the SP must provide a fully comprehensive and functional indexing service for all new documents coming under its management.

Searching for hard copy and electronic records

The SP must have systems and processes in place to enable it to accurately search and identify the location of hard copy and electronic records within the timeframes of the SLA and any relevant legislation.

The SP must ensure it holds electronic indexes for each database, therefore all searches will be checking against an electronic index.

These systems must catalogue all records held and their location, either the physical location in the case of hard copy records or logical location in the case of electronic records.

The SP must be able to search for records, hard copy and electronic, using key identifiers. These will vary depending on the index, but should include at a minimum the following - name, date of birth and NI number.

The SP must also be able to use a string of key words to search to locate records, in particular where key identifiers have not been provided.

Where a key word search is being completed the SP must be able to provide a list of the results electronically to the requester.

If the SP cannot locate the record through searching the indexes (no trace), they must not go on to charge a retrieval fee for that record.

The SP must restrict the use of indexing and search tools to trained and authorised personnel only.

The search tool used by the SP must display the total number of hits from a search on the User's screen and must allow the User to then display the search results (the "hit list"), or refine the search criteria and issue another request.

Indexing hard copy records

As part of searching for the records, the SP must ensure it has indexed the records in line with the requirements below.

Both the physical location of all boxes containing hard copy records and the contents of those boxes must be recorded and kept up-to-date in a suitable system. The SP must be able to search effectively on that system.

Indexing electronic records

The search tool must allow electronic records, files etc. listed in a hit list to be selected and then opened (subject to access controls) by a single click or keystrokes.

Updating the records index

As part of searching and retrieving records the SP must create necessary database entries in respect of records at the following times:

- as records are deposited in the record stores;
- as records are transferred;
- as records are re-filed;
- as records are retrieved;
- as records are permanently withdrawn;
- as records are returned to the records store by Users; and
- on disposal.

Once entries for particular records exist on a database, the SP must keep these entries up-to-date as part of its normal service. For the avoidance of doubt updates to the index will not be charged separately.

The SP must ensure that any new records created are filed according to the standards governing the existing records.

If requested by CLU, the SP must create an electronic copy of any document brought under its management by scanning the document. It is expected that this will be minimal in volume.

The SP must restrict the ability to update the indexation to authorised and trained personnel only.

The SP must maintain a complete record of modifications made to any records (e.g. addition, amendment or destruction of any documentation).

In the case of record packs for a claim that is not yet settled, the SP must ensure that the claimant's solicitor is notified of any change made to the record pack and provided with an up-to-date version of the record pack in CD version or other electronic format as directed by CLU.

The SP must ensure that any modifications to existing records are reflected in the records index within one working day of the update being made.

New hard copy deposits – indexing and filing

The SP must provide a fully comprehensive and functional indexing service for all new hard copy records coming under its management.

The SP must ensure that the new records are filed into storage in line with the storage requirements.

The SP must ensure that all new hard copy deposits are filed accurately.

The SP must ensure that all new records will be brought into the appropriate records store within one week of CLU's notification of the requirement, unless a schedule is otherwise agreed with CLU.

## Retrieval, distribution & delivery and put aways

Following the receipt of a request for access to data , the SP must search for and locate the requested documentation, as per the requirements of section 5. Requests for information received can result in hard copy, electronic copy or a combination being sent to the requester. Once a search has been conducted as a result of a request, the SP must retrieve hard copy records from the storage location. The SP must then make a copy of the requested document. This can either be by photocopying or scanning the document, according to the requester's preferred format. The request is then completed when the copied document(s) has been sent to the requester and the requester has acknowledged receipt.

There are instances when original documentation may be dispatched as a result of a request for information, usually when a Court requests that original documentation be provided in evidence. Such requests will normally be handled via CLU's external solicitors. If original documentation is ever moved from a storage location the SP must ensure its safe passage to the recipient, in accordance with Government data handling guidelines, and to maintain a full audit trail of any movement until it has been delivered.

As well as retrieving and distributing hard copy records, the SP will also receive records back. The SP must ensure that the records received back are "put away" in a locatable storage place. The SP must ensure that it indexes and puts away the record. For the avoidance of doubt, the SP will charge one fee under put aways to incorporate indexing and the physical act of putting the record away.

There is a requirement for the SP to be able to prepare and send files to TNA. The SP must follow the guidance clearly set out by TNA.

Service Requirements for retrieval, distribution & delivery and put aways

Retrieval

The SP must have the processes in place to physically retrieve hard copy records from the storage facilities and also processes to retrieve electronic records. The SP must ensure that the picking of hard copy records, or the operation of any machinery used to facilitate this process, is performed only by authorised personnel.

The SP must record in monthly MI when there is a “no trace” if a physical check was conducted to attempt to find a record. A no trace would mean that there was a positive search complete but no records could be found in the hard copy environment.

The SP must ensure that all original documentation removed from its storage location for the purpose of processing an information request (e.g. scanning or photocopying) is returned in its original state to the correct storage location once the requested documentation has been dispatched.

The SP must ensure that the exact location of all hard copy records is updated in the electronic search and location tool. This includes full visibility of the location of a

record from the time it is picked from its storage location until its return to that location.

The SP must ensure that a full audit trail is maintained of all hard copy records that have been retrieved, and of which hard or electronic copies have been made. The SP must maintain a process which allows CLU's claims handlers to access requested record packs through a web portal.

Distribution and delivery

The SP must prepare hard and electronic records for distribution. This will include providing the hard copy and electronic records in the format required by the requester. For example, the requester may require hard copy records in the original, photocopy or scanned image format.

The SP must be able to distribute records electronically, hard copy records via a secure delivery service, encrypted CDs via a secure delivery service, records via a secure encrypted email system or any other such secure method as proposed by the SP and agreed by CLU such as web portals.

The SP must have the capability to distribute and protect records with PROTECT markings during the lifetime of this contract.

The SP must put in place a process for distribution which will include photo- copying hard copy records where appropriate and/or copying the records to an electronic medium. The SP must provide photocopying facilities allowing high quality copies of original hard copy records to be made as part of distributing the records. The photocopying must be completed using appropriately trained staff.

The SP must be able to render all of the types of electronic records specified by the organisation in a manner that preserves the information on the records, and in line with retention periods set out by CLU, (for example, all the features of visual presentation and layout produced by the generating application package), and which renders all components of an electronic record together.

The SP must ensure that copies of electronic records can be printed and dispatched in hard copy by a registered courier, if so requested.

The SP must ensure that requested records can be downloaded to password protected encrypted portable media (e.g. USB stick, CD, DVD etc.) in line with Cabinet Office guidance and dispatched via registered courier if so requested . The use of portable media should be kept to a minimum, particularly for bulk records.

The SP must put in place a process to ensure the safe delivery of the records. The SP will be regarded as completing an information request either in hard copy or electronic, when the requester notifies the SP of receipt of the records.

For all record pack requests received from the claims handlers, the request will be considered completed once the requested documents are available to the claims handlers, and the claims handlers have been informed of this.

The SP must ensure that only documents or data that have been requested, and which the requester is entitled to access, are dispatched and it must demonstrate it has procedures in place to achieve this.

The SP must only use registered post, in-house vans or CLU approved couriers when dispatching copies of any records, either hard copy or electronic copy written to removable media. If the records are protectively marked, these records must be handled in accordance with the protocols governing the protective marking. The SP must be able to track the records at all points.

When transferring Personal Data by removable media such as CD/DVD/USB, the SP must ensure this is completed by password encrypted means and arrangements made to notify the approved recipient of the password. CLU requires that all removable media containing personal information must be encrypted, in line with Cabinet Office guidance. The SP must ensure that passwords are strong.

The SP must ensure removable media is encrypted to at least current Cabinet Office standards or equivalent in addition to being protected by an authentication mechanism, such as a strong password.

The SP must include a copy of the original request when dispatching documentation as evidence that the request has been successfully completed.

The SP must ensure that original documentation is moved only in dedicated secured containers and approved vehicles if it is being moved away from its storage location.

The SP must obtain confirmation of delivery from the recipient for any original documentation that is moved away from a storage location in the form of a delivery note and retain such records for 12 months.

The SP must implement procedures to ensure that all original documentation is fully traceable at all stages of a journey if moved from its secure storage location.

The SP must record any original documentation that has been moved off site, its intended recipient and the date of dispatch.

The SP must take steps to locate original documentation which has been off site for 3 months and return it to its long-term storage location or otherwise agree a period of

further retention with the record holder. Where required, extensions must be discussed and agreed with CLU.

Put Aways

Where hard copy records are returned to the SP, they must ensure that the index

systems are updated, and the records accurately put away into storage.

The SP must seek to utilise the most efficient space when putting away records.

TNA preparation

The SP must offer a service for cleaning records/files before dispatch to TNA, to be taken up at the CLU's option. Records for transfer to TNA will have been identified by CLU.

The SP must follow the guidance set out by TNA regarding the preparation and packing of files. The full guidance can be found here and covers standards relating to:

- Removal of all corrosive metal, staples pins;
- Repair of torn or damaged page edges;
- Removal and destruction of duplicate pages;
- Transfer of photographs to specialist sleeves; and
- Replacement of damaged covers with new, acid free covers.

The SP must follow the requirements set out by TNA regarding cataloguing the records, which can be found here.

There may be a requirement in the future to provide electronic records to TNA. If this is required it is expected that the SP will provide a new price.

## Projects

### Background to projects

As part of the ongoing business as usual work set out in the contract, there may be additional pieces of work required from the SP which are larger in scale. It is envisaged that these 'projects' are an extension of core services which are just larger in scale and greater in volume than normal day to day business. It is anticipated that all projects will encompass elements of the core services, for example a 'Disclosure Project' will entail searching, retrieval and distribution functions.

At this point in time, there are no such projects planned. CLU would normally expect to alert the SP to likely project work in the regular contract meetings and seek to give as much advance notice as possible. That said, urgent projects cannot be ruled out.

It is not expected that many projects will necessitate services outside what is defined in the core services. However, if the project is of a significant magnitude or complexity which requires additional resources e.g. project management, then these proposals must be submitted via the contract variation route.

### Service Requirements for projects

The SP must be able to complete any projects as though they are core services.

The SP must be able to demonstrate the ability to provide flexible services in line with

changing requirements.

## Data Handling

The SP must be responsible not only for the management and safeguarding of the physical and electronic records under its management as set out above, but also for the data contained in those records. It is essential that the SP works with the CLU and its stakeholders to handle data securely. This data must be managed in line with the relevant legislation. Many of these records contain personal information for the

former British Coal employees. This includes such information as names, current and past addresses, date of birth and National Insurance numbers.

In addition to the potential risks posed to claimants detailed above, all of these records are the property of CLU and form part of the national public record. Until such time as CLU decides that these records can be disposed of, the SP is required to keep them secure and prevent unauthorised access.

- Cause substantial distress to individuals;
- Breach proper undertakings to maintain the confidence of information to third parties; and
- Breach statutory restrictions on the disclosure of information.

There are also a number of other records which are UNRESTRICTED, such as records relating to mining activity and administration records. These records do not require the same treatment as personal records but must still be managed responsibly.

Objectives for data handling

- All Personal Data processed by the SP on behalf of the CLU is processed in compliance with the DPA.
- To ensure that CLU and the SP comply with the requirements of handling data to the guideline set out for PROTECT – PERSONAL, including doing everything possible to:

i. Make accidental compromise or damage unlikely during storage, handling, use, processing, transmission or transport;
ii. Deter deliberate compromise or opportunistic attack; and
iii. Dispose of or destroy in a manner to make reconstruction unlikely.

- Ensure that data under the SP's management does not come into the possession or view of unauthorised persons, organisations or other third parties.
- Ensure that the integrity of data under its management is maintained at all times.
- Ensure that any breaches in data security are reported through the appropriate channels to CLU and any other appropriate Governmental Department or Agency.
- Ensure that processes and procedures used by the SP to store and manage CLU data are designed and operate effectively, ensuring that the security and integrity of this data is maintained at all times.

Service Requirements for data handling

- The SP must ensure that all of its record storage and retrieval policies comply fully with all relevant UK and EU regulations.
- The SP must support CLU in its compliance with the DPA when processing Personal Data.

- The SP must produce a Security Plan.
- The SP must maintain an appropriate infrastructure, procedural and resource framework to ensure that the Personal Data held by the SP, for which CLU is responsible, is managed in compliance with the DPA at all times.
- The SP must have adequate technical and organisational measures in place to prevent unauthorised and unlawful processing of Personal Data and accidental loss or destruction of, or damage to, Personal Data.
- The SP must take steps to ensure that those staff processing Personal Data on behalf of CLU are adequately trained and made aware of their roles and responsibilities.
- The SP must operate to defined procedures and organisational controls for monitoring and reporting all incidents involving Personal Data. The SP must have a process in place to identify, log and report immediately all unauthorised and

unlawful processing of Personal Data and accidental loss or destruction of, or damage to, Personal Data to CLU.

Confidentiality – Internal to the SP

- The SP must ensure that a confidentiality undertaking in a form agreed with CLU governing the handling of records is signed by the SP and all of the SP's staff employed in the records service.
- The SP must maintain a written record of all personnel who have signed the Confidentiality Undertaking.
- The SP must make the written record referred to above available to CLU on request.
- The SP must allow the CLU to complete an IT health check of all systems provided prior to going live and perform annual checks thereafter.
- The SP must allow the CLU to ensure all IT systems are accredited prior to going live and periodically reviewed to maintain annual accreditation thereafter.
- The SP must provide the CLU with an annual compliance statement from the SP's account manager.
- The SP must ensure that there is a least a minimum level of information risk awareness training provided to all staff with access to Personal Data.
- The SP must ensure that all SP personnel with access to records undergo CLU approved training on appointment and at least annually to understand the varying levels of confidentiality that must be adhered to for different record and document types.
- The SP must use logical security tools to restrict access to electronic records to appropriate personnel. At a minimum, all electronic databases and indexing systems must be password protected with access also controlled by user access rights.
- The SP must restrict access to records to those users who require it to perform their job functions.
- The SP must ensure that any electronic records transferred to removable media are encrypted to the relevant Government standard in addition to being protected by an authentication mechanism, such as a strong password.

- The SP must put in place arrangements to log the activity of data users in respect of electronically held personal information, and for managers to check that there arrangements are being properly adhered to.
- The SP must refrain from making unnecessary copies of PROTECT marked assets, and should only pass copies to people who have a need to know the information and are approved by CLU.
- The SP must have incident response processes and procedures in place.
- CLU reserves the right to engage a third party organisation to perform a periodic security review of the SP's security compliance and the SP must provide all necessary assistance to facilitate this.

Confidentiality – External to the SP

- The SP must only grant users access to records according to the class of user.
- The SP must ensure that medical records stored by the SP are made available only to the individual to whom the records refer, CLU or any third parties who have been granted express written permission by either the individual or CLU.

- The SP must seek CLU's explicit written authorisation to proceed with any access request not covered by the contract between SP and CLU.
- The SP must not move any original CLU records off-site for any reason without receiving prior written authorisation from CLU.
- The SP must encrypt any data transferred as part of a backup to a remote secure location.
- The SP must protect any networks on which electronic data is stored using firewalls acquired and configured to reflect best commercial practice.
- The SP must use firewalls and other means as necessary to prevent the unintentional electronic transfer of any CLU records.
- The SP must ensure that no protective marking or descriptor is shown on any external envelope containing PROTECT marked assets.

Sending data abroad

- The SP must only transfer data abroad and not process data abroad.
- The SP must ensure that, when sending data abroad, the level of encryption employed will be at least equivalent to that set out for the UK, unless there is a legal restriction on encryption in the receiving country. In this case advice must be obtained from CLU on a suitable method of transfer.

Data security breaches

The SP must implement a policy for reporting, managing and recovering from information risk incidents, including the loss of protected Personal Data and Information and Communication Technology ("ICT") security incidents, define responsibilities, and make staff aware of this policy.

The SP must inform CLU within 1 working day in the event of a loss of data or

suspected security breach of any kind, and then follow the instructions received from CLU.

The SP must provide details of the exact nature of any such event, including:

- the type of information and number of records;

- the circumstances of the loss / release / corruption;
- action taken to minimise / mitigate effect on individuals involved, including whether they have been informed;
- details of how the breach is being investigated;
- whether any other regulatory body has been informed and their response;
- remedial action taken to prevent future occurrence; and
- any other information the SP feels may assist CLU or other governmental agencies in making an assessment.

The SP must take all reasonable action to prevent the further loss of data on identification of a possible breach of data security.

## Scanning

The SP must be able to provide scanning facilities if required by CLU. However, it is likely that the amount of scanning required will be extremely small.

Objectives for scanning

- To provide, or have access to, facilities capable of scanning any hard copy documentation under the SP's management over the life of the contract.
- The SP must meet the current guidelines for the legal admissibility of scanned documents where these records could be required. It may not be necessary to meet this high standard for documents which do not need to be legally admissible.
- The SP must use all reasonable endeavours to ensure in all cases that the image is legible, and the SP must put in place quality assurance processes to achieve this.
- The SP must ensure that the integrity of hard copy records is maintained and not impacted upon by the physical act of scanning documents.

## Destruction

CLU has a duty to ensure that all records with "PROTECT" marking or treated as "PROTECT" are disposed of properly. The disposal of records is defined as the point in their lifecycle when they are either transferred to archives (TNA/County Archives) or destroyed.

Objectives for destruction

- Ensure records that meet the criteria of the "PROTECT" classification level, which are no longer required to be retained, are destroyed in a secure manner in compliance with agreed service levels and that no information is inadvertently disclosed.
- Ensure compliance with all applicable legal and regulatory requirements.
- Ensure that the disposal of information assets (includes paper and electronic documents as well as all computer systems and devices that have been used to process or hold CLU information) has been carried out according to an agreed policy and the retention schedule, and that this disposal can be evidenced.
- All records are appropriately disposed of at the end of their retention period.
- Ensure that destruction is undertaken promptly once approval has been given by CLU and records are not destroyed unless approved by CLU.
- No adverse incidents occurred regarding the security of the record during disposal.

Requirements

The SP must have organisational controls, procedures and resources to ensure that all records are disposed of in accordance with the agreed procedures and in accordance with CLU's records retention and disposal schedule.

The SP must provide a system for documenting appraisal decisions (all decisions on destruction will be made by the CLU Records Review Panel). Members of the group should include but are not limited to CLU, CMS, the SP and TNA. This should include information on records selected for permanent preservation, destroyed or retained by CLU.

The SP must ensure records selected for permanent preservation are transferred to a deep storage facility of the SP.

The SP must ensure records not selected for permanent preservation and which have reached the end of their administrative life, are destroyed in a secure manner as soon as is possible.

The SP must produce monthly disposal reports for paper and electronic records outlining the audit trail of the destruction of records showing their reference, description and date of destruction and the method of destruction.

Hard copy records

The SP must carry out the destruction of all hard copy data whilst at all time ensuring confidentiality is safeguarded at every stage of the destruction process.

The SP must ensure that details of the destroyed records are recorded.

Electronic data

The SP must ensure that electronic data will be subject to the same disposal decision process and controls as hard copy records.

The SP must ensure that steps are taken to ensure that the destruction of any physical media on which electronic data is stored is managed so that no data can be reconstructed from the physical media.

## IT Requirements

The SP must provide a resilient IT infrastructure to ensure minimal downtime in the event of software or hardware failure. This must also include appropriate levels of backup and recovery procedures and processes, all of which must be in place and fully tested by the SP by the start of the contract.

The SP must provide sufficient IT skills and numbers of support resources to undertake the day to day running of the IT systems and infrastructure.

The SP must provide arrangements to undertake any Systems Transfer and Data Migration together with the ongoing technical support to ensure all SLAs are met. The SP must ensure robust systems are in place to back up all data on a regular basis to minimise the risk of loss in the event of failure of the primary system. The SP must ensure that it executes an annual data disaster recovery exercise, including a full system restore of data. This should also include a recovery log detailing:

- Recovery media ID;
- Date of restore;
- Name of system restored;
- Number of files restored;

- Size of data restore; and
- Number of files that failed restore and reason for failure.

The SP must provide to CLU details of the proposed backup policy and procedure.

IT refresh

The SP must ensure that all elements of the IT infrastructure, including all hardware, operating systems and anti-virus applications, together with any core software applications used to store CLU data, are fully maintained and supported at all times to a level consistent with securing good VFM. For clarity, this means:

- hardware must be fully maintained by the SP and be capable of supporting the software and data capacities. In addition, it must provide
- adequate performance for the number of users accessing the system; and
- the operating system and any application software used for the system must be fully maintained at all times. For example, if an operating system is no longer supported by the supplier then it must be upgraded to the next supported version. The same is expected of any application software. Where it is no longer supported, it must be upgraded to the next supported version.

This requirement does not preclude the SP from upgrading if they see a performance or other advantage in moving to new hardware or application software. However, as with any change, this must be agreed in advance with CLU based on a costed

business case and supporting justification to be provided by the SP as part of the Change Control Procedure.

The issue of interdependencies must also be considered when upgrading a particular component. For example, when an operating system is upgraded this would likely have additional consequences on the application software. It could also have an impact on the hardware in that it may not be capable of running the new version.

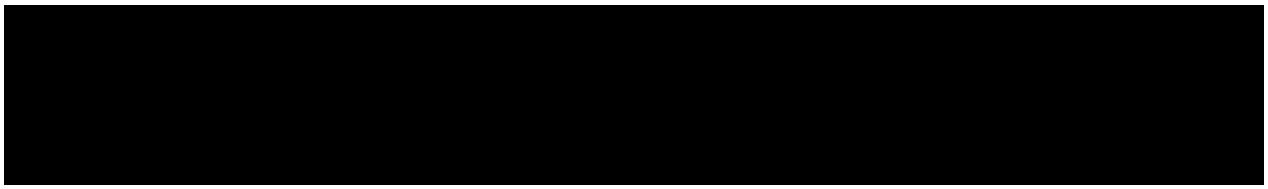
## Transition

For the contract to be fully operational by 1 June 2024, it is essential that the SP plans a period of transition which is discussed and agreed in advance with the CLU. The SP must work collaboratively with CLU to ensure a timely and smooth transition. CLU expects collaboration between the SP and the incumbent supplier to achieve this.

Should there be any variation to the indicative timeline then discussions will happen between the 3 parties to ensure that the 1st June date is not compromised.

The hard copy records are often decades old, and some have deteriorated with time. The need to relocate all of these documents, coupled with their current condition, will result in an increased risk of the documents being damaged or lost. There is also a risk that moving them will result in a misalignment between their location as recorded in the various indexing systems, and their physical location at current and future storage locations.

The successful SP must ensure that effective measures are taken to ensure that records are not damaged, misplaced or that the accuracy of the current indexing systems is not affected by the need to move these documents as part of the transition phase.



All system hardware is currently owned by the incumbent. The SP must therefore, as part of the IT infrastructure, provide the necessary server hardware, operating systems, anti-virus, and backup software required to run all systems transferred as part of the requirement.

It is expected that there will be a staged approach to transition as the CLU need to be confident that there will be access to ongoing records during this phase. The CLU could be in the process of a large-scale disclosure exercise during the transition phase which would require hard copy and electronic records to be located and sent to other parties such as legal advisers.

Objectives for transition

- To ensure that all records and data are relocated from their current storage locations by the start of the contract. This covers both the movement of physical records and electronic records.
- To ensure that the integrity of all data, both hard copy and electronic, is maintained at all stages of the transition process.
- To ensure that the records and data under the SP's management do not come into the possession or view of unauthorised persons, organisations or third parties during the transition process.
- To ensure that the effectiveness and accuracy of the current indexing system is not reduced during, or as a result of, the transition process.
- To ensure that an infrastructure is in place capable of receiving all of the existing electronic data, and that skilled personnel are available to process this transfer.
- To ensure that all records can still be located and retrieved if required during the transition process.
- To ensure that the SP maintains its governance arrangements during transition including, inter alia, MI and risk reporting, assets inventory, business continuity & disaster recovery plans, service manual and invoice process.

Transition Requirements

As part of the response to this ITT, the bidders must respond with a high level plan describing how they would manage transition. The detailed plan will be subsequently agreed by CLU with the successful SP before the transition can begin. The SP must set out transition costs as part of the Pricing Schedule.

The SP must set out how it would manage the transition period, taking into account the requirements set out in this section, and set out the associated costs, transition plan, prior relevant experience and a summary of the lessons learnt.

The SP must provide CLU with regular updates on the progress of the transition, in a format to be stipulated by CLU prior to the start of the transition.

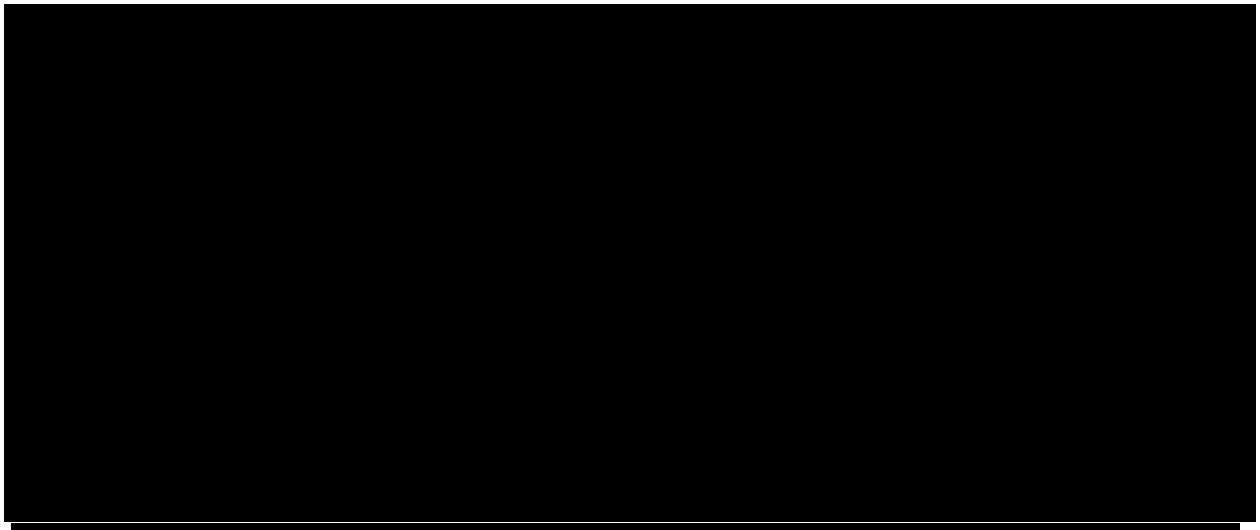
The SP must ensure that only trained personnel with a clear understanding of their roles and responsibilities are employed at all stages of transition.

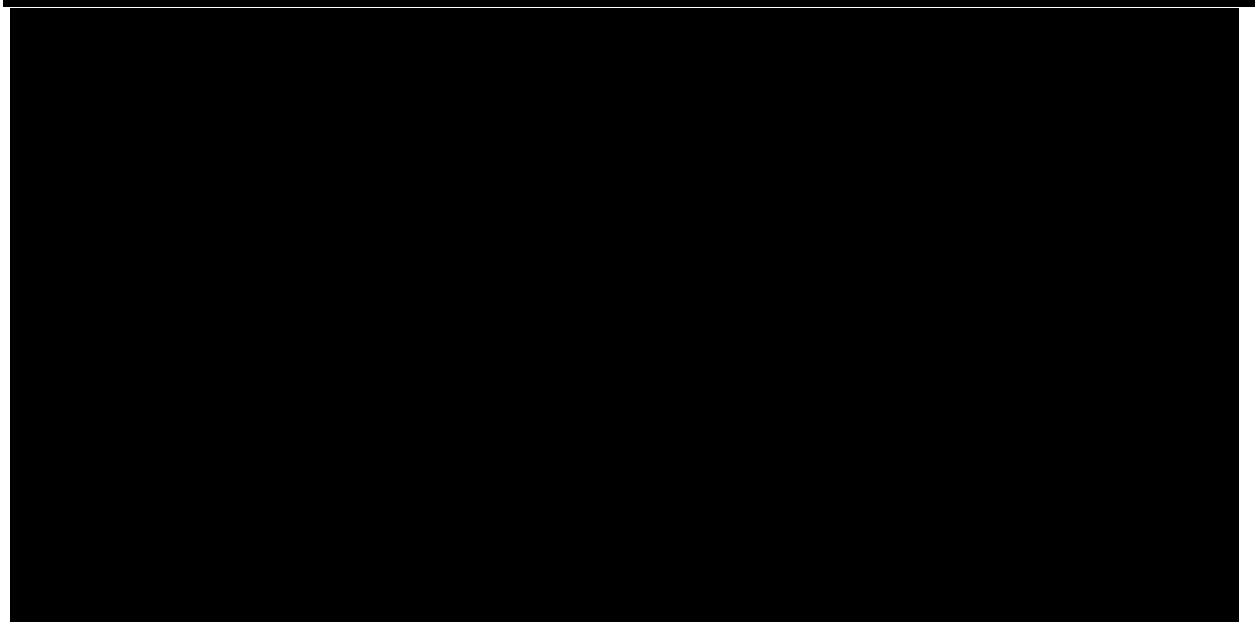
The SP must allow and co-operate with an audit of the transition phase, to be conducted at any stage during or after transition by CLU or an authorised third party.

The SP must provide CLU, at the end of transition, with written and signed assurances that the transition has been successfully completed.

The SP must ensure that all records are locatable at all times during transition and must not allow transition activities to have an adverse impact on CLU's operations.

The SP must work constructively with both the current incumbent and other third parties such as legal advisers and the claims handlers throughout transition to enable them to meet their responsibilities.





IT Transition

The SP must transfer, migrate and manage the IT systems that support the storage, searching and retrieval of all CLU physical and electronic records within the terms of this contract. To achieve this, the SP must provide a scalable infrastructure together with an appropriate level of personnel required to enable the efficient transfer of the current IM systems and data.

At the start of the contract, the SP must provide as part of the transition process, a full transition plan and data audit plan.

The SP must state their preferred strategy for the migration of data.

The SP must provide a data and audit migration strategy to ensure complete and accurate migration of all data to the new environment.

The SP must ensure that access to records is always maintained during migration. As well as a migration strategy, the SP must provide a migration plan, migration schedule and regression plans. These should be discussed and agreed with CLU prior to any migration.

It is expected that the SP must perform data profiling prior to the migration. In addition, the SP must audit the data both pre and post-migration and reconcile the output to show evidence of successful migration.

The SP must demonstrate an awareness of the adherence to industry best practice with the use of tools to support the Data Migration.

As part of the Data Migration, the SP must ensure User involvement and agree and sign off Data Migration requirements, acceptance tests and schedules with CLU prior to executing any Data Migration.

The SP must ensure that the authenticity, accuracy and integrity of the migrated data

is maintained.

The SP must provide CLU with regular updates during the migration exercise.

## Exit Management

Background to exit management

It is vital for CLU to have an effective exit management strategy agreed with the SP. As this is intended to be a long term relationship, CLU needs to be able to provide assurance to HM Treasury and others that there will not be any unexpected exit costs at the end of the contract. CLU may also be required to demonstrate to external parties such as the NAO that there is a clear process in place for managing the exit from the contract.

For the avoidance of doubt, CLU will not pay all of the SP's costs in relation to exit management.

The SP must provide and implement an exit management plan which is agreed by both parties. Exit management will be completed between all three parties: CLU; the SP; and a future SP. The plans must provide a smooth transition out of the contract. As a minimum, the plan must contain information on:

- all activities needed in the transfer of the services from the SP to any potential new contractor within timescales directed by CLU;
- individual activities relating to the SP and how they will be exited;
- staff;
- assets;
- premises;
- licenses and Intellectual Property Rights;
- data and records, including confidential information belonging to CLU;
- communications between stakeholders; and

- MI.

The SP must provide suitable resource to manage the exit process.

The SP must deliver to CLU all documentation and systems for the continuing delivery of the services within the contract.

The SP must ensure access to the records is maintained during the exit process.

The SP must ensure no loss of information during the exit process.

The SP must ensure that there are processes in place to transfer the services set out in the contract to any potential new contractor.

The SP must cooperate fully with CLU and the new contractor throughout the exit management process.

The SP must provide regular updates and MI to CLU.

The SP must ensure that disruption to normal contract service is kept to a minimum.

The SP must provide a lessons learned report to CLU on the contract.

The SP must identify risks and issues affecting the exit and assist CLU with mitigating these risks.

**DOCUMENT 3**

**EVALUATION CRITERIA AND SCORING METHODOLOGY**

**1. Evaluation Criteria**

DESNZ will select the applicant that provides the most economically advantageous bid to be its preferred supplier. Tenders will be evaluated by at least three staff associated with the project.

The scores will be as follows:

0 Unacceptable – meets none of the requirement

1 Unsatisfactory – well below the requirement

2 Weak – below requirement

3 Adequate – mostly meets the requirement

4. Good – completely meets the requirement with moderate levels of assurance

5 –Excellent – completely meets the standard with high levels of assurance

For scored questions a weighting showing the relative importance of each is given. Your score for each question from each evaluator will be ascertained by multiplying the score awarded by the applicable weighting. Your total score will be the aggregate of the weighted scores awarded by all of the evaluators.

**2. Evaluation Questions**

**Technical Sections – total weighting 65%**

For each question, as well as providing your proposal, please demonstrate previous success by providing examples. Your answer to each question must be no more than 4 pages A4 in length. Any answers over this length will be disregarded.

Q1. How will you ensure electronic and hard copy records are stored securely and preserved so as to avoid deterioration, corruption, damage or loss? Weighting 25%

Q2. How will you ensure that required response times for provision of data are met? Weighting 25%

Q3. How will you ensure that data is shared appropriately? Weighting 25%

Q4. How will you respond to any future change in requirements? Weighting 15%

Q5. How will ensure ongoing value for money? Weighting 10%

**Social Value Section – total weighting 10%**

Please refer to the Social Value Model Award Criteria (MAC) guidelines for further information.

Q6. Fighting climate change – weighting 50%

Describe the commitment your organisation will make to ensure that opportunities under the contract deliver the Policy Outcome and Award Criteria for MAC 4.1 - *Deliver additional environmental benefits in the performance of the contract including working towards net zero greenhouse gas.*

Q7. Tackling economic inequality – weighting 50%

Describe the commitment your organisation will make to ensure that opportunities under the contract deliver the Policy Outcome and Award Criteria for MAC 2.2 - *Create employment and training*

*opportunities particularly for those who face barriers to employment and/or who are located in deprived areas, and for people in industries with known skills shortages or in high growth sectors*.

**Pricing Section – total weighting 25%**

Please submit a firm and fixed yearly bid price for the Service. You should include a detailed breakdown of your costs.

Price will be scored as follows:

Prices will be scored via the 'Price per quality point' method (PQP).

In this approach a PQP is calculated for each bid by:

- determining the bid price;
- determining the quality score for each bid, expressed as a whole number rather than as a percentage (though the whole number may still be points out of 100); and
- dividing the bid price by the quality score to give an output price per quality point.

Price

Quality score

The number arrived at is the PQP.

**DOCUMENT 4**

**PROPOSED CONTRACT TERMS AND CONDITIONS IN ACCORDANCE WITH THE CROWN COMMERCIAL SERVICE FRAMEWORK**

**See attached Annex 2 for proposed Draft T&Cs**

**DOCUMENT 5**

**DECLARATIONS**

**Statement of non collusion**

To The Department for Energy & Industrial Strategy

1. We recognise that the essence of competitive tendering is that the Department will receive a bona fide competitive tender from all persons tendering. We therefore certify that this is a bona fide tender and that we have not fixed or adjusted the amount of the tender or our rates and prices included therein by or in accordance with any agreement or arrangement with any other person.

2. We also certify that we have not done and undertake not to do at any time before the hour and date specified for the return of this tender any of the following acts:

(a) communicate to any person other than the Department the amount or approximate amount of our proposed tender, except where the disclosure, in confidence, of the approximate amount is necessary to obtain any insurance premium quotation required for the preparation of the tender;

(b) enter into any agreement or arrangement with any other person that he shall refrain for submitting a tender or as to the amount included in the tender;

(c) offer or pay or give or agree to pay or give any sum of money, inducement or valuable consideration directly or indirectly to any person doing or having done or causing or having caused to be done, in relation to any other actual or proposed tender for the contract any act, omission or thing of the kind described above.

3. In this certificate, the word “person” shall include any person, body or association, corporate or unincorporated; and “any agreement or arrangement” includes any such information, formal or informal, whether legally binding or not.

Signature (duly authorised on behalf of the tenderer)

Print name

On behalf of (organisation name)

Date

**Form of Tender**

To The Department for Energy & Industrial Strategy

1. Having considered the invitation to tender and all accompanying documents (including without limitation, the terms and conditions of contract and the Specification) we confirm that we are fully satisfied as to our experience and ability to deliver the goods/services in all respects in accordance with the requirements of this invitation to tender.

2. We hereby tender and undertake to provide and complete all the services required to be performed in accordance with the terms and conditions of contract and the Specification for the amount set out in the Pricing Schedule.

3. We agree that the framework terms and conditions shall apply.

4. We agree that this tender shall remain open to be accepted by the Department for 4 weeks from the date below.

5. We understand that if we are a subsidiary (within the meaning of section 1159 of (and schedule 6 to) the Companies Act 2006) if requested by the Department we may be required to secure a Deed of Guarantee in favour of the Department from our holding company or ultimate holding company, as determined by the Department in their discretion.

6. We understand that the Department is not bound to accept the lowest or any tender it may receive.

0. We certify that this is a bona fide tender.

Signature (duly authorised on behalf of the tenderer)

Print name

On behalf of (organisation name)

Date

# CALL-OFF SCHEDULE 24

These Iron Mountain InSight® Services terms and conditions (these "**Terms and Conditions**") are in addition to the CONTRACT and shall govern the provision of InSight Services (which together shall form the "**Agreement**"). COMPANY and CONTRACTOR are each referred to as a "**Party**" and collectively, the "**Parties**.". If there are any conflict between the Terms and Conditions and the CONTRACT, the Terms and Conditions shall take precedence in relation to the provision of Insight Services

**1. DEFINITIONS.** Capitalized terms shall have the meanings set forth in this section, or in the section where they are first used.

"**Access Protocols**" means the usernames, passwords, access codes, encryption keys, service accounts, technical specifications, connectivity standards or protocols, or other relevant procedures, as may be necessary to allow COMPANY to access the Services.

[redacted]

"**Authorized User**" means any individual who is an employee of COMPANY or such other person as may be authorized by COMPANY to access the InSight Services pursuant to COMPANY's rights under these Terms and Conditions. An Authorized User is granted access using the COMPANY-owned identity provider ("**IDP**") or through an CONTRACTOR- managed IDP.

"**COMPANY Data**" means all content, data and information that is input or uploaded to, or collected, received, processed, or stored in the InSight Services by or on behalf of COMPANY, and all derivative data thereto, including but not limited to derivative data created in accordance with an SOW. For the avoidance of doubt, COMPANY Data does not include Usage Data or any other information reflecting the access or use of the InSight Services by or on behalf of COMPANY or any Authorized User.

"**Documentation**" means the user manuals, training materials, reference guides, instruction materials, help files and similar documentation provided by CONTRACTOR or its suppliers to COMPANY in hard copy or electronic form or available on CONTRACTOR's online portal describing the use, operations, features, functionalities, user responsibilities, procedures, commands, requirements, limitations and capabilities of and/or similar information about the Services.

"**Encrypted**" or "**encrypted**" shall mean data that has been rendered through algorithmic transformation or any other means available into an unrecognizable form in which meaning cannot be understood without the use of a confidential process or key.

"**High Risk Activities**" means uses such as, without limitation, the operation of nuclear facilities, air traffic control, or life support systems, where the use or failure of the Services could lead to death, personal injury, or environmental damage.

"**Implementation Services**" means the implementation services documented in an SOW relating to the InSight Services, including service details related to IDP integration, security controls and special accommodations, which require CONTRACTOR assistance to implement.

"**InSight Services**" means the CONTRACTOR InSight hosted SaaS solution, as described in a Statement of Work.

"**Intellectual Property Rights**" means any and all now known or hereafter existing: (a) rights associated with works of authorship, including copyrights, mask work rights, and moral rights; (b) trademark or service mark rights; (c) trade secret rights; (d) patents, patent rights, and industrial property rights; (e) layout design rights, design rights, and other proprietary rights of every kind and nature other than trademarks, service marks, trade dress, and similar rights; and (f) all registrations, applications, renewals, extensions, or reissues of the foregoing, in each case in any jurisdiction throughout the world.

"**CONTRACTOR ML**" means CONTRACTOR's machine learning and artificial intelligence technology including all modifications, derivative works and improvements thereto developed by either Party or a third party.

"**Professional Services**" means the training, customization, Implementation Services, data ingestion, consulting or other services CONTRACTOR or its suppliers may perform for the benefit of COMPANY in connection with the InSight Services as described as Professional Services in a Statement of Work.

"**Services**" means the InSight Services, Professional Services and Support Services, as may be set forth in a Statement of Work.

"**Services Technology**" means the software, databases, platforms, and other technologies used by or on behalf of CONTRACTOR in performing the Services, whether operated directly by CONTRACTOR or through the use of third-party services.

**"Service Term"** means the initial term of COMPANY's authorized use of the Services, as set forth in the applicable Statement of Work, together with any renewal terms. The initial term begins on the earlier of: (i) the date COMPANY starts using or receiving the Services; or (ii) the effective date set out in the Statement of Work.

"**Statement of Work**" or "**SOW**" means a document that: (a) contains details regarding the Services to be performed or provided, including pricing and other specifics, (b) is mutually agreed upon and executed by the Parties, and (c) incorporates these Terms and Conditions to form the Agreement.

"**Support Services**" means the support services and related maintenance for the InSight Services purchased by COMPANY as described in a Statement of Work.

"**Usage Data**" means any diagnostic and usage-related information from the use, performance and operation of the InSight Services, including, but not limited to, type of browser, Service features, and systems that are used and/or accessed, and system and Service performance-related data.

**2. PROVISION OF SERVICES**

**2.1 Services Use.** Subject to and conditioned on COMPANY's and its Authorized Users' compliance with these Terms and Conditions, CONTRACTOR hereby grants COMPANY a non-exclusive, non-transferable right, during the Term, solely for COMPANY's internal business purposes and in accordance with the limitations and restrictions contained herein, to: (a) access and use the InSight Services in accordance with these Terms and Conditions and the Documentation; and (b) use the Documentation solely to support COMPANY's use of the InSight Services. CONTRACTOR may change or modify the Documentation and Services, including adding or removing features and functions, from time to time, provided that in no event will such modifications materially reduce the functionality provided to COMPANY during the Term.

**2.2 Access Protocols.** CONTRACTOR will provide the Services to COMPANY at the rates and charges set forth in the applicable Statement(s) of Work. CONTRACTOR will work with the COMPANY to provide access through the Access Protocol implementation process, including providing COMPANY with training on user account setup and access control implementation with the applicable IDP. COMPANY is solely responsible for obtaining and maintaining its equipment, computers, networks, and communications, including Internet access, required to access and utilize the Services and for all expenses related thereto. CONTRACTOR is not responsible for any issues relating to access attributable to COMPANY or any third party. COMPANY agrees to maintain and update an industry standard anti-virus program within its computer systems that are used in connection with the Services.

**2.3 Authorized Users.** COMPANY may designate its Authorized Users and grant their access rights to the features and functions of the InSight Services. Usernames and passwords ("**User IDs**") cannot be shared or used by more than one Authorized User at a time. Depending on the agreed login and authorization implementation, CONTRACTOR may assist the COMPANY with establishing User IDs for COMPANY's Authorized User who has been designated as a "User Manager" and provide such User Manager with rights to create, control and manage its portfolio of Authorized Users, including, but not limited to, the number of Authorized Users and all User IDs, in accordance with the Access Protocols. COMPANY shall not disclose or make available User IDs or other Access Protocols other than to COMPANY's Authorized Users and shall prevent unauthorized access to, or use of, the InSight Services, and will notify CONTRACTOR promptly of any actual or suspected unauthorized use. COMPANY is solely responsible for management of the User IDs, access rights and the acts and omissions of its Authorized Users. COMPANYs shall immediately terminate an Authorized User's access to InSight Services if such individual is no longer employed or engaged by COMPANY, engages in inappropriate activity, or is otherwise no longer authorized to have access. COMPANY is responsible for ensuring all Authorized Users comply with COMPANY's obligations under these Terms and Conditions. CONTRACTOR reserves the right to: (a) track and review user profiles, access and activity at any time; and (b) terminate any User ID that it reasonably determines may have been used in a way that breaches this Section 2.3.

**2.4 Professional Services.** CONTRACTOR will provide Professional Services as may be mutually agreed to by the Parties from time to time and set forth in a Statement of Work. Each Statement of Work will be governed by these Terms and Conditions. CONTRACTOR shall have the right to remove, reassign, or take any other employment related action in regard to any of its personnel furnished to provide Professional Services. In the event of such removal or reassignment, CONTRACTOR will furnish a replacement of similar skills and capability. CONTRACTOR reserves the right to hire temporary workers or subcontractors to perform the service, provided

those workers possess the skills required to perform the Professional Services.

**3. INTELLECTUAL PROPERTY**

**3.1 Ownership.** Subject to Section 3.4 (Open Source Software), the Services, Documentation, Usage Data, and all other materials provided by CONTRACTOR hereunder, including but not limited to all manuals, , reports, records, programs, information, and data (that is not COMPANY Data or COMPANY's Intellectual Property thereto), together with all know-how, enhancements, modifications, corrections, improvements, adaptations, new applications, and derivative works relating to the same, derived from the same or created in connection with the same, and all worldwide Intellectual Property Rights in each of the foregoing (**"IM Materials"**), are the exclusive property of CONTRACTOR and its suppliers. To the extent any rights in the Services, Documentation or Usage Data vest in COMPANY, COMPANY hereby unconditionally and irrevocably assigns to CONTRACTOR any and all such rights, title and/or interest including Intellectual Property Rights relating thereto. All rights in and to IM Materials not expressly granted to COMPANY under the Agreement are reserved by CONTRACTOR and its suppliers. Except as expressly set forth herein, no express or implied license or right of any kind is granted to COMPANY regarding the IM Materials or any part thereof, including any right to obtain possession of any source code, data or other technical material related to the Services. Nothing hereunder shall act so as to assign or otherwise transfer COMPANY's ownership of COMPANY Data to any other party.

**3.2 License; Ownership.** COMPANY Data hosted by CONTRACTOR as part of the Services, and all worldwide Intellectual Property Rights in such data, are the exclusive property of COMPANY. COMPANY grants CONTRACTOR and its suppliers an irrevocable, non-exclusive, worldwide, royalty-free and fully paid-up license to access, use, reproduce, modify, display, process and store the COMPANY Data for purposes of providing the Services to the COMPANY. Moreover, if training CONTRACTOR ML is expressly contemplated in an SOW, CONTRACTOR may access, use, reproduce, copy, modify, internally display, process, store, or otherwise create derivative works of COMPANY Data to build, train and maintain the CONTRACTOR ML used to provide the Services. CONTRACTOR may freely use and license CONTRACTOR ML, provided that CONTRACTOR will remove COMPANY Data in CONTRACTOR ML or otherwise, after expiration or termination of the Agreement, and will not otherwise share such data with other customers. All rights in and to the COMPANY Data not expressly granted to CONTRACTOR in the Agreement are reserved by COMPANY. Under these Terms and Conditions, the Parties acknowledge and agree that CONTRACTOR is a data processor and service provider.

**3.3 Restrictions on Use.** COMPANY shall not permit any party to access or use the Services, Services Technology or Documentation, other than the Authorized Users. Except as expressly permitted by these Terms and Conditions, COMPANY agrees that it will not, and will not permit any of its Authorized Users or other party to: (a) copy, modify, adapt, alter or translate, in whole or in part, or create derivative works of, the Services Technology, Documentation or any component thereof; (b) license, sublicense, sell, resell, lease, rent, loan, timeshare, transfer, assign, distribute, disclose or otherwise commercially exploit or make available, in whole or in part, the Services, Services Technology or Documentation to any third party; (c) reverse engineer, decompile, disassemble (except to the extent applicable laws specifically prohibit such restriction), decode, adapt or otherwise in any manner attempt to obtain, create or recreate, derive or attempt to derive, determine or gain access to the source code (or the underlying ideas, algorithms, structure or organization) of the Services, Services Technology, Documentation or any component thereof, in whole or in part, except to the extent expressly permitted by applicable law (and then only upon advance written notice to CONTRACTOR); (d) disclose or transmit any information regarding the Services, Services Technology or Documentation to any individual other than an Authorized User,; (e) use or access the Services, Services Technology or Documentation for competitive analysis or to build a similar product; (f) use the Services, Services Technology or any component thereof: (I) to send or store infringing, threatening, harassing, defamatory, libelous, obscene, pornographic, indecent or otherwise unlawful or tortious material, including material harmful to children or violating third party privacy rights, (II) to send or store material containing software viruses, worms, Trojan horses or other harmful computer code, files, scripts, agents or programs, (III) for High Risk Activities, (IV) in any manner or for any purpose that infringes, misappropriates, or otherwise violates any Intellectual Property Rights or other right of any person or that violates any applicable law, or (V) to benefit any third party (other than an Authorized User) or otherwise incorporate the same into a product or service COMPANY provides to a third party (other than Authorized Users); (g) perform benchmarking analysis or disclose the results of any benchmark test of

Services, Services Technology or Documentation to any third party; (h) interfere with or disrupt the integrity or performance of the Services, Services Technology or the data contained therein; (i) access, use or share any data other than COMPANY Data; (j) bypass or breach any security device or protection used for or contained in the Services or Services Technology or otherwise attempt to gain unauthorized access to the Services, Services Technology or its related systems or networks, or otherwise circumvent mechanisms intended to limit use; (k) remove, erase, modify, tamper, obscure, or fail to preserve any proprietary, copyright or other notices; or (l) unless expressly agreed to in a relevant SOW, let, encourage or assist any third party, automated software, robotic process automation, scraper or other tool to do any of the foregoing (a)-(k).

**3.4 Open Source Software.** CONTRACTOR shall take commercially reasonable measures to ensure that the Services and any other materials provided to COMPANY as part of the Services, unless expressly agreed to otherwise in writing by COMPANY, will not contain software that is made available by a third party under a free or open source software licensing model, if such model: (i) creates or purports to create contribution obligations with respect to any COMPANY software, or (ii) grants or purports to grant to any third party any rights to such COMPANY software ("**FOSS**"). To the extent any such FOSS is included in the Services, such FOSS is licensed under the terms of such third party license model and additional obligations may apply. CONTRACTOR distributes and passes through such terms and conditions of such FOSS licenses to COMPANY to the extent necessary to comply with any such license obligations . Nothing in these Terms and Conditions enlarges or curtails COMPANY's rights under, or otherwise grants COMPANY rights that supersede, the terms and conditions of any applicable FOSS license.

**3.5 Feedback.** If COMPANY provides CONTRACTOR any feedback or suggestions about the Services, Services Technology or Documentation (the "**Feedback**"), then CONTRACTOR may use such information without obligation to COMPANY, and COMPANY hereby irrevocably assigns all rights, title and interest in the Feedback to CONTRACTOR.

**4. COMPANY RESPONSIBILITIES**

**4.1 COMPANY Warranty.** COMPANY represents and warrants that, to the extent COMPANY or COMPANY's third party provides COMPANY Data for the purposes herein: (a) it is the owner or legal custodian of the COMPANY Data; (b) it has given all necessary notices and obtained all necessary consents, authorizations and/or legal permissions required to direct and enable CONTRACTOR and its suppliers to access, use and process the COMPANY Data as set forth in these Terms and Conditions and the related Statement(s) of Work; (c) will use the Services in accordance with all applicable data, privacy and security laws; and (d) any COMPANY Data hosted by CONTRACTOR as part of the Services shall not (i) infringe any copyright, trademark, or patent; (ii) misappropriate any trade secret; (iii) be defamatory, obscene, pornographic or unlawful; (iv) contain any viruses, worms or other malicious computer programming codes intended to damage CONTRACTOR's systems or data; or (v) otherwise violate the rights of a third party or violate any applicable law. CONTRACTOR is not obligated to back up any COMPANY Data. COMPANY agrees that any use of the Services contrary to or in violation of the representations and warranties of COMPANY in this Section constitutes unauthorized and improper use of the Services. COMPANY will immediately notify CONTRACTOR of any issues of which it becomes aware that could negatively impact CONTRACTOR's ability to process the COMPANY Data in accordance with these Terms and Conditions.

**4.2 COMPANY Responsibility for Data and Security.** COMPANY and its Authorized Users shall have access to the COMPANY Data and shall be responsible for any and all: (a) changes to and/or deletions of COMPANY Data, maintaining the security and confidentiality of all User IDs and other Access Protocols required in order to use and access the InSight Services; (b) activities that occur in connection with such use and access. CONTRACTOR and its suppliers are not responsible or liable for (i) the deletion of or failure to store any COMPANY Data by COMPANY or its Authorized Users; (ii) determining whether the security of the environment provided by CONTRACTOR is commensurate with its needs, and (iii) long term backup copies of COMPANY Data. Notwithstanding the foregoing CONTRACTOR will maintain resiliency and redundancy processes associated with the InSight Services to meet industry standards for storage of COMPANY Data. COMPANY is responsible for any long term backup or archival of the COMPANY Data that is provided to

CONTRACTOR. CONTRACTOR shall maintain service accounts and encryption keys on behalf of the COMPANY necessary to perform the Services. CONTRACTOR shall not be liable to COMPANY for a failure to maintain relevant service accounts and encryption keys if such failure is due to COMPANY's lack of cooperation or failure to assist in the provision of access to COMPANY Data. To the extent COMPANY or COMPANY's third party provides COMPANY Data for the purposes herein, COMPANY shall have the sole responsibility for the accuracy, quality, integrity, legality, reliability, and appropriateness of all COMPANY Data, and for ensuring that it complies with the AUP, and CONTRACTOR and its suppliers reserve the right to review the COMPANY Data for compliance with the AUP. In no event will CONTRACTOR be liable for any loss of COMPANY Data, or other claims arising out of or in connection with the unauthorized acquisition or use of Access Protocols.

**4.3 Cooperation.** COMPANY agrees to provide CONTRACTOR with such cooperation, materials, information, access and support, which CONTRACTOR deems reasonably required to allow CONTRACTOR to successfully provide the Services. COMPANY understands and agrees that the success of the Services is contingent upon COMPANY providing such cooperation, materials, information, access and support.

**4.4 Data Transmittal.** To the extent COMPANY transmits any electronic COMPANY Data to or from CONTRACTOR and/or the InSight Services, COMPANY shall transmit any such COMPANY Data in accordance with the acceptable methods and requirements for data transmittal set forth in a Statement of Work or Documentation. All such COMPANY Data transmitted to or from CONTRACTOR must use secure and encrypted protocols. COMPANY assumes full responsibility to safeguard against unauthorized access and to encrypt its electronic COMPANY Data prior to and during the transmission and transfer of its electronic COMPANY Data to and from CONTRACTOR.

**5. DATA HOSTING**

[redacted]

**6. CONFIDENTIALITY**

**6.1 Confidential Information.** Under the Agreement each Party (the "**Disclosing Party**") may provide the other Party (the "**Receiving Party**") with certain information regarding the Disclosing Party's business, technology, products, or services or other confidential or proprietary information, and which is marked as "confidential" or "proprietary" or would normally under the circumstances be considered confidential information (collectively, "**Confidential Information**"). COMPANY Data will be considered Confidential Information of COMPANY, and the Services, Services Technology, Documentation, Usage Data and all enhancements and improvements thereto, as well as these Terms and Conditions and any SOW details, will be considered Confidential Information of CONTRACTOR.

**6.2 Protection of Confidential Information.** The Receiving Party agrees that it will: (a) not disclose to any third party any Confidential Information of the Disclosing Party, except: (i) to its Affiliates, directors, employees, agents, suppliers or subcontractors who have agreed to restrictions similar to those set forth in this Section 6 to the extent such disclosure is necessary for the performance of the Agreement or (ii) as may be required by law; (b)

not use any Confidential Information of the Disclosing Party except for the purposes contemplated by these Terms and Conditions and the related Statement(s) of Work; and (c) protect the Disclosing Party's Confidential Information from unauthorized use, access, or disclosure in the same manner that it protects its own confidential and proprietary information of a similar nature, but in no event with less than reasonable care.

**6.3 Exceptions.** The confidentiality obligations set forth in this section will not apply to any information that: (a) becomes generally available to the public through no fault of the Receiving Party; (b) is lawfully provided to the Receiving Party by a third party free of any confidentiality duties or obligations; (c) was already known to the Receiving Party at the time of disclosure; or (d) the Receiving Party can prove, by clear and convincing evidence, was independently developed by employees and contractors of the Receiving Party who had no access to the Confidential Information. In addition, the Receiving Party may disclose Confidential Information to the extent that such disclosure is necessary for the Receiving Party to enforce its rights under these Terms and Conditions or is required by law, governmental regulation, court order, subpoena, warrant, governmental regulatory or agency request, or other valid legal authority, legal procedure or similar process ("**Legal Process**"), provided that the Receiving Party uses commercially reasonable efforts to promptly notify the Disclosing Party in writing of such required disclosure unless the Receiving Party is informed that: (i) it is legally prohibited from giving notice; or (ii) the Legal Process relates to exceptional circumstances involving danger of death or serious physical injury to any person. The Receiving Party will cooperate with the Disclosing Party if the Disclosing Party seeks an appropriate protective order. Notwithstanding anything to the contrary in this Section 6, should either Party learn some general information regarding the other Party's Confidential Information during the Term or any relevant Trial Period, the Party learning such information is free to use that information retained in its unaided memory, without specific or intentional memorization or reference to such Confidential Information, for its own business purposes (including but not limited to such Party's employee skill, knowledge, talent, and/or expertise on other or future projects), *except* to the extent such information is the other Party's Intellectual Property. Receipt of Confidential Information hereunder, however in no way obligates the Receiving Party to monitor or limit its employees' work.

## 7. WARRANTIES AND DISCLAIMERS

**7.1 Limited Services Warranty.** CONTRACTOR warrants to COMPANY that the Services will materially conform with the Documentation and to the extent Professional Services are provided, such Services will be performed using reasonable care and skill. In the event of CONTRACTOR's breach of the foregoing warranties, COMPANY's exclusive remedy and CONTRACTOR's sole liability will be for CONTRACTOR to use commercially reasonable efforts to repair or replace such Services, or in the instance of Professional Services to re-perform the Professional Services, at no charge to COMPANY. **COMPANY acknowledges that the accuracy of any predictive models utilized in providing the Services is dependent on both the volume and quality of the data used to build the models. CONTRACTOR gives no warranty as to the accuracy, correctness, or completeness in live operation of any such predictive model used by the Services or predictions made by the Services.**

**7.2 Disclaimer. The limited warranty set forth in Section 7.1 is made for the benefit of COMPANY only. Except as expressly provided in Section 7.1 and to the maximum extent permitted by applicable law, CONTRACTOR and its suppliers make no (and hereby disclaim all) other warranties, whether written, oral, express, implied or statutory, including, without limitation, any implied warranties of satisfactory quality, course of dealing, trade usage or practice, merchantability, non-infringement, or fitness for a particular purpose. The Services are provided "as is" and neither CONTRACTOR nor its suppliers warrant that all errors or defects can be corrected, or that operation of the Services shall be uninterrupted or error-free. The Services are not designated or intnded for High Risk Activities.**

## 8. TERM AND TERMINATION

**8.1 Termination for Changes to Applicable Law or Supplier Relationship.** Either Party may terminate the Agreement upon written notice to the other Party if: (a) the relationship and/or the transactions contemplated in a Statement of Work would violate any applicable law; or (b) if an agreement between CONTRACTOR and

a supplier ("**Supplier Agreement**") expires or terminates or a supplier discontinues any portion or feature of the services supplier provides pursuant to a Supplier Agreement, resulting in CONTRACTOR's inability to provide the applicable Services to COMPANY in whole or in part.

**8.2 Suspension of Services by CONTRACTOR.** CONTRACTOR may suspend or limit COMPANY's or any Authorized User's use of the Services provided subject to these Terms and Conditions (including, without limitation, its transmission or retrieval of COMPANY Data) immediately upon written notice to COMPANY, without liability, for any one of the following reasons: (a) COMPANY fails to pay any undisputed fees as and when due pursuant to these Terms and Conditions or the applicable Statement of Work and such failure continues for a period of thirty (30) days; (b) the Services are being used by COMPANY or any of its Authorized Users in violation of any applicable federal, state or local law, ordinance or regulation; (c) the Services are being used by COMPANY or any of its Authorized Users in an unauthorized manner; (d) COMPANY's or any of its Authorized User's use of the Services violates the AUP, adversely affects CONTRACTOR's provision of services to other customers or poses a security risk to CONTRACTOR's systems; or (e) a court or other governmental authority having jurisdiction issues an order prohibiting CONTRACTOR from furnishing the Services to COMPANY. During any such suspension, COMPANY shall remain responsible and liable for all fees due for the suspended Services. If any of the foregoing grounds for suspension continues for more than fifteen (15) days, CONTRACTOR shall have the right to terminate the Agreement for cause and without an opportunity to cure by COMPANY.

**8.3 Effect of Termination.** If the Agreement expires or is terminated for any reason, then: (a) COMPANY's rights to access and use the Services shall immediately terminate; (b) all fees owed by COMPANY to CONTRACTOR will be immediately due upon receipt of the final invoice; (c) CONTRACTOR and the COMPANY shall delete all COMPANY Data from the InSight Services no later than thirty (30) days from the termination or expiration date of the Agreement; and (d) upon request, each Party will use commercially reasonably efforts to return or delete all Confidential Information of the other Party, provided that, for clarity, CONTRACTOR's obligations under this Section not apply to any Usage Data. In the event that COMPANY Data remains on the InSight Services on the Host after the expiration or termination of the Agreement, these Terms and Conditions and all fees shall continue to apply until all COMPANY Data has been removed from the Host. The sections and subsections titled *Definitions, Restrictions on Use, Confidentiality, Warranties and Disclaimers, Limitation of Liability, Indemnification, Effect of Termination*, and *Miscellaneous* will survive expiration or termination of the Agreement for any reason.