Schedule 6 – Change Control Procedure

1 The Parties acknowledge that minor changes to the Contract may be necessary to reflect operational and administrative procedures during the Term and that such minor changes may be agreed in writing between the Parties' respective contract managers.

2 The Contractor shall use reasonable endeavours to incorporate minor changes requested by the DFE within the current Charges and shall not serve a Contractor Notice of Change unless the change involves a demonstrable material increase to its costs or requires a material change to the Contract.

3 Either Party may request a Variation provided that such Variation does not amount to a material change.

4. The DFE may request a Variation by completing the Change Control Note and giving the Contractor sufficient information to assess the extent of the Variation and consider whether any change to the Charges are required in order to implement the Variation within a reasonable time limit specified by the DFE. If the Contractor accepts the Variation it shall confirm it in writing within 21 days of receiving the Change Control Note.

5. If the Contractor is unable to accept the Variation or where the Parties are unable to agree a change to the Charges, the DFE may allow the Contractor to fulfil its obligations under the Contract without Variation or if the Parties cannot agree to the Variation the Dispute will be determined in accordance with clause 36.

6. If the Contractor wishes to introduce a change to the Contract it may request a Variation by serving the Change Control Note on DFE.

7. The DFE shall evaluate the Contractor's proposed Variation in good faith, taking into account all relevant issues.

8. The DFE shall confirm in writing within 21 days of receiving the Change Control Note if it accepts or rejects the Variation.

9. The DFE may at its absolute discretion reject any request for a Variation proposed by the Contractor.

Change Control Note:

Contract Number:		**DFE Contract / Programme Manager:**	
Contractor:		**Original Contract Value:**	
Contract Start Date:		**Contract Expiry Date:**	

Variation Requested:	
Originator of Variation: (tick as appropriate)	DfE ☐ Contractor ☐
Date:	
Reason for Variation:	
Summary of Variation: (e.g. specification, finances, contract period)	
Date of Variation commencement:	
Date of Variation expiry : (if applicable)	
Total Value of Variation: (if applicable)	
Payment Profile: (if applicable)	
Revised daily rate: (if applicable)	
Impact on original contract: (if applicable)	
Supporting Information: (please attach all supporting documentation for this Change Control)	
Terms and Conditions:	Save as herein amended all other terms and conditions of the Original Contract shall remain in full force and effect.

Variation Agreed	
For the Contractor:	**For the DFE:**
Signature.....	**Signature**.....
Full Name.....	**Full Name**.....
Title.....	**Title**.....
Date.....	**Date**.....

Please note that no works/services described in this form should be undertaken, and no invoices will be paid until both copies of the CCN are signed, returned and counter-signed.

To be entered by the Commercial department:			
Commercial Contact:		**Reference Number:**	
Date received:		**EC Reference:**	

Schedule 7 – Key Personnel and Key Sub Contractors

Key Personnel

The individuals listed in the table below are Key Personnel:

Name	Role	Period of Involvement
[redacted]		

Key Sub-Contractors

The Contractor may sub-contract its obligations under the Contract to the Sub-Contractors listed in the table below.

Sub-contractor Name	Registered Office and Company Number	Related Product/Service Description	Sub-contract Value[3]	Role in delivery of the Services

[3] Expressed as a percentage of total projected Charges over Term

Schedule 8 – Data, Systems Handling and Security

Definitions

"Control"	means that a person possesses, directly or indirectly, the power to direct or cause the direction of the management and policies of the other person (whether through the ownership of voting shares, by contract or otherwise) and **"Controls"** and **"Controlled"** are interpreted accordingly;
"Data Loss Event"	any event that results, or may result, in unauthorised access to Personal Data held by the Processor under this Contract, and/or actual or potential loss and/or destruction of Personal Data in breach of this Contract, including any Personal Data Breach.
"DPA"	Data Protection Act 2018
"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"	(i) the GDPR, the LED and any applicable national implementing Laws as amended from time to time (ii) the DPA 2018 [subject to Royal Assent] to the extent that it relates to processing of personal data and privacy; (iiii) all applicable Law about the processing of personal data and privacy;
"Data Subject 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.
"Controller", "Processor," "Data Subject", "Personal Data", "Personal Data Breach", "Data Protection Officer"	shall have the meanings given in the GDPR;
"GDPR"	the General Data Protection Regulation (Regulation (EU) 2016/679)
"Law"	means 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 Processor is bound to comply;
"LED"	Law Enforcement Directive (Directive (EU) 2016/680)
"Processor Personnel"	employees, agents, consultants and contractors of the Processor and/or of any Sub-Processor engaged in the performance of its obligations under this Contract.
"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 set out in the Contract.
"Sub-processor"	any third Party appointed to process Personal Data on behalf of the Processor related to this Contract

1.1 The Parties acknowledge that for the purposes of the Data Protection Legislation, the Customer is the Controller and the Contractor is the Processor unless otherwise specified in Schedule 8 Annex 2. The only processing that the Processor is authorised to do is listed in Schedule 8 Annex 2 by the Controller and may not be determined by the Processor

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

1.3 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 operations and the purpose of the processing;

(b) an assessment of the necessity and proportionality of the processing operations in relation to the Services;

(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.

1.4 The Processor shall, in relation to any Personal Data processed in connection with its obligations under this Contract:

(a) process that Personal Data only in accordance with Schedule 8 Annex 2 , unless the Processor is required to do otherwise by Law. If it is so required the Processor shall promptly notify the Controller before processing the Personal Data unless prohibited by Law;

(b) ensure that it has in place Protective Measures, which are appropriate to protect against a Data Loss Event, 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 Data Loss Event;

(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 this Contract (and in particular Schedule 3a);

(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 clause;

(B) are subject to appropriate confidentiality undertakings with the Processor or any Sub-processor;

(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 this Contract; and

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

(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;

(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.

1.5 Subject to clause 1.6, the Processor shall notify the Controller immediately if it:

(a) receives a Data Subject Request (or purported Data Subject 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 this 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 Data Loss Event.

1.6 The Processor's obligation to notify under clause 1.5 shall include the provision of further information to the Controller in phases, as details become available.

1.7 Taking into account the nature of the processing, the Processor shall provide the Controller with full assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under clause 1.5 (and insofar as possible within the timescales reasonably required by the Controller) including by promptly 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 the Controller to comply with a Data Subject 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 Data Loss Event;

(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.

1.8 The Processor shall maintain complete and accurate records and information to demonstrate its compliance with this clause. 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; and

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

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

1.10 Each Party shall designate its own data protection officer if required by the Data Protection Legislation.

1.11 Before allowing any Sub-processor to process any Personal Data related to this Contract, the Processor must:

(a) notify the Controller in writing of the intended Sub-processor and processing;

(b) obtain the written consent of the Controller;

(c) enter into a written agreement with the Sub-processor which give effect to the terms set out in this clause 1 such that they apply to the Sub-processor; and

(d) provide the Controller with such information regarding the Sub-processor as the Controller may reasonably require.

1.12 The Processor shall remain fully liable for all acts or omissions of any Sub-processor.

1.13 The Controller may, at any time on not less than 30 Working Days' notice, revise this clause 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 this Contract).

1.14 The Parties agree to take account of any guidance issued by the Information Commissioner's Office. The Controller may on not less than 30 Working Days' notice to the Processor amend this Contract to ensure that it complies with any guidance issued by the Information Commissioner's Office.

Schedule 8 – Annex 1

DFE SECURITY STANDARDS

"BPSS" **"Baseline Personnel Security Standard"**	a level of security clearance described as pre-employment checks in the National Vetting Policy. Further information can be found at: https://www.gov.uk/government/publications/government-baseline-personnel-security-standard
"CCSC" **"Certified Cyber Security Consultancy"**	is NCSC's approach to assessing the services provided by consultancies and confirming that they meet NCSC's standards. This approach builds on the strength of CLAS and certifies the competence of suppliers to deliver a wide and complex range of cyber security consultancy services to both the public and private sectors. See website: https://www.ncsc.gov.uk/scheme/certified-cyber-consultancy
"CCP" **"Certified Professional"**	is a NCSC scheme in consultation with government, industry and academia to address the growing need for specialists in the cyber security profession and are building a community of recognised professionals in both the UK public and private sectors. See website: https://www.ncsc.gov.uk/scheme/certified-professional
"CC" **"Common Criteria"**	the Common Criteria scheme provides assurance that a developer's claims about the security features of their product are valid and have been independently tested against recognised criteria.
"CPA" **"Commercial Product Assurance"** formerly called "CESG Product Assurance"	is an 'information assurance scheme' which evaluates commercial off the shelf (COTS) products and their developers against published security and development standards. These CPA certified products can be used by government, the wider public sector and industry. See website: https://www.ncsc.gov.uk/scheme/commercial-product-assurance-cpa
"Cyber Essentials" **"Cyber Essentials Plus"**	Cyber Essentials is the government backed, industry supported scheme to help organisations protect themselves against common cyber-attacks. Cyber Essentials and Cyber Essentials Plus are levels within the scheme. There are a number of certification bodies that can be approached for further advice on the scheme; the link below points to one of these providers: https://www.iasme.co.uk/apply-for-self-assessment/
"Department's Data" **"Department's Information"**	is any data or information owned or retained in order to meet departmental business objectives and tasks, including: (a) any data, text, drawings, diagrams, images or sounds

	(together with any repository or database made up of any of these components) which are embodied in any electronic, magnetic, optical or tangible media, and which are: (i) supplied to the Contractor by or on behalf of the Department; or (ii) which the Contractor is required to generate, process, store or transmit pursuant to this Contract; or (b) any Personal Data for which the Department is the Data Controller;
"DfE"	means the Department for Education
"Department"	
"Departmental Security Standards"	means the Department's security policy or any standards, procedures, process or specification for security that the Contractor is required to deliver.
"Digital Marketplace / GCloud"	the Digital Marketplace is the online framework for identifying and procuring cloud technology and people for digital projects. Cloud services (e.g. web hosting or IT health checks) are on the G-Cloud framework.
"FIPS 140-2"	this is the Federal Information Processing Standard (FIPS) Publication 140-2, (FIPS PUB 140-2), entitled 'Security Requirements for Cryptographic Modules'. This document is the de facto security standard used for the accreditation of cryptographic modules.
"Good Industry Practice" **"Industry Good Practice"**	means the exercise of that degree of skill, care, prudence, efficiency, foresight and timeliness as would be expected from a leading company within the relevant industry or business sector.
"Good Industry Standard" **"Industry Good Standard"**	means the implementation of products and solutions, and the exercise of that degree of skill, care, prudence, efficiency, foresight and timeliness as would be expected from a leading company within the relevant industry or business sector.
"GSC" **"GSCP"**	means the Government Security Classification Policy which establishes the rules for classifying HMG information. The policy is available at: https://www.gov.uk/government/publications/government-security-classifications
"HMG"	means Her Majesty's Government
"ICT"	means Information and Communications Technology (ICT) is used as an extended synonym for information technology (IT), used to describe the bringing together of enabling technologies used to deliver the end-to-end solution

"ISO/IEC 27001" "ISO 27001"	is the International Standard for Information Security Management Systems Requirements
"ISO/IEC 27002" "ISO 27002"	is the International Standard describing the Code of Practice for Information Security Controls.
"ISO 22301"	is the International Standard describing for Business Continuity
"IT Security Health Check (ITSHC)" **"IT Health Check (ITHC)"** **"Penetration Testing"**	means an assessment to identify risks and vulnerabilities in systems, applications and networks which may compromise the confidentiality, integrity or availability of information held on that IT system.
"Need-to-Know"	the Need-to-Know principle is employed within HMG to limit the distribution of classified information to those people with a clear 'need to know' in order to carry out their duties.
"NCSC"	The National Cyber Security Centre (NCSC) formerly CESG is the UK government's National Technical Authority for Information Assurance. The NCSC website is https://www.ncsc.gov.uk
"OFFICIAL" **"OFFICIAL-SENSITIVE"**	the term 'OFFICIAL' is used to describe the baseline level of 'security classification' described within the Government Security Classification Policy (GSCP) which details the level of protection to be afforded to information by HMG, for all routine public sector business, operations and services. the 'OFFICIAL–SENSITIVE' caveat is used to identify a limited subset of OFFICIAL information that could have more damaging consequences (for individuals, an organisation or government generally) if it were lost, stolen or published in the media, as described in the Government Security Classification Policy.
"Secure Sanitisation"	Secure sanitisation is the process of treating data held on storage media to reduce the likelihood of retrieval and reconstruction to an acceptable level. Some forms of sanitisation will allow you to re-use the media, while others are destructive in nature and render the media unusable. Secure sanitisation was previously covered by "Information Assurance Standard No. 5 - Secure Sanitisation" ("IS5") issued by the former CESG. Guidance can now be found at: https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media The disposal of physical documents and hardcopy materials advice can be found at: https://www.cpni.gov.uk/secure-destruction
"Security and Information Risk Advisor" **"CCP SIRA"** **"SIRA"**	the Security and Information Risk Advisor (SIRA) is a role defined under the NCSC Certified Professional (CCP) Scheme. See also:

	https://www.ncsc.gov.uk/articles/about-certified-professional-scheme
"SPF" **"HMG Security Policy Framework"**	This is the definitive HMG Security Policy which describes the expectations of the Cabinet Secretary and Government's Official Committee on Security on how HMG organisations and third parties handling HMG information and other assets will apply protective security to ensure HMG can function effectively, efficiently and securely. https://www.gov.uk/government/publications/security-policy-framework
"Tailored Assurance" formerly called "CTAS", or, "CESG Tailored Assurance"	is an 'information assurance scheme' which provides assurance for a wide range of HMG, MOD, Critical National Infrastructure (CNI) and public sector customers procuring IT systems, products and services, ranging from simple software components to national infrastructure networks. https://www.ncsc.gov.uk/documents/ctas-principles-and-methodology

1.1 The Contractor shall comply with Departmental Security Standards for Contractors which include but are not constrained to the following clauses.

1.2 Where the Contractor will provide ICT products or services or otherwise handle information at OFFICIAL on behalf of the Department, the requirements under Cabinet Office Procurement Policy Note – Use of Cyber Essentials Scheme certification - Action Note 09/14 25 May 2016, or any subsequent updated document, are mandated; that "contractors supplying products or services to HMG shall have achieved, and retain certification at the appropriate level, under the HMG Cyber Essentials Scheme". The certification scope must be relevant to the services supplied to, or on behalf of, the Department.

1.3 The Contractor shall be able to demonstrate conformance to, and show evidence of such conformance to the ISO/IEC 27001 (Information Security Management Systems Requirements) standard, including the application of controls from ISO/IEC 27002 (Code of Practice for Information Security Controls).

1.4 The Contractor shall follow the UK Government Security Classification Policy (GSCP) in respect of any Departmental Data being handled in the course of providing this service, and will handle this data in accordance with its security classification. (In the event where the Contractor has an existing Protective Marking Scheme then the Contractor may continue to use this but must map the HMG security classifications against it to ensure the correct controls are applied to the Departmental Data).

1.5 Departmental Data being handled in the course of providing an ICT solution or service must be segregated from all other data on the Contractor's or sub-contractor's own IT equipment to protect the Departmental Data and enable the data to be identified and securely deleted when required. In the event that it is not possible to segregate any Departmental Data then the Contractor and any sub-contractor shall be required to ensure that it is stored in such a way that it is possible to securely delete the data in line with Clause 1.14.

1.6 The Contractor shall have in place and maintain physical security, in line with those outlined in ISO/IEC 27002 including, but not limited to, entry control mechanisms (e.g. door access) to premises and sensitive areas

1.7 The Contractor shall have in place and maintain an access control policy and process for the logical access (e.g. identification and authentication) to ICT systems to ensure only authorised personnel have access to Departmental Data.

1.8 The Contractor shall have in place and shall maintain procedural, personnel, physical and technical safeguards to protect Departmental Data, including but not limited to: physical security controls; good industry standard policies and process; anti-virus and firewalls; security updates and up-to-date patching regimes for anti-virus solutions; operating systems, network devices, and application software, user access controls and the creation and retention of audit logs of system use.

1.9 Any data in transit using either physical or electronic transfer methods across public space or cyberspace, including mail and couriers systems, or third party provider networks must be protected via encryption which

has been certified to FIPS 140-2 standard or a similar method approved by the Department prior to being used for the transfer of any Departmental Data.

1.10 Storage of Departmental Data on any portable devices or media shall be limited to the absolute minimum required to deliver the stated business requirement and shall be subject to Clause 1.11 and 1.12 below.

1.11 Any portable removable media (including but not constrained to pen drives, flash drives, memory sticks, CDs, DVDs, or other devices) which handle, store or process Departmental Data to deliver and support the service, shall be under the control and configuration management of the contractor or (sub-)contractors providing the service, shall be both necessary to deliver the service and shall be encrypted using a product which has been certified to FIPS140-2 standard or another encryption standard that is acceptable to the Department.

1.12 All portable ICT devices, including but not limited to laptops, tablets, smartphones or other devices, such as smart watches, which handle, store or process Departmental Data to deliver and support the service, shall be under the control and configuration management of the contractor or sub-contractors providing the service, and shall be necessary to deliver the service. These devices shall be full-disk encrypted using a product which has been certified to FIPS140-2 standard or another encryption standard that is acceptable to the Department.

1.13 Whilst in the Contractor's care all removable media and hardcopy paper documents containing Departmental Data must be handled securely and secured under lock and key when not in use and shall be securely destroyed when no longer required, using either a cross-cut shredder or a professional secure disposal organisation.

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

1.15 At the end of the contract or in the event of equipment failure or obsolescence, all Departmental information and data, in either hardcopy or electronic format, that is physically held or logically stored on the Contractor's ICT infrastructure must be securely sanitised or destroyed and accounted for in accordance with the current HMG policy using a NCSC approved product or method. Where sanitisation or destruction is not possible for legal, regulatory or technical reasons, such as a Storage Area Network (SAN) or shared backup tapes, then the Contractor or sub-contractor shall protect the Department's information and data until the time, which may be long after the end of the contract, when it can be securely cleansed or destroyed.

1.16 Access by Contractor or sub-contractor staff to Departmental Data shall be confined to those individuals who have a "need-to-know" in order to carry out their role; and have undergone mandatory pre-employment screening, to a minimum of HMG Baseline Personnel Security Standard (BPSS); or hold an appropriate National Security Vetting clearance as required by the Department. All Contractor or sub-contractor staff must complete this process before access to Departmental Data is permitted.

1.17 All Contractor or sub-contractor employees who handle Departmental Data must have annual awareness training in protecting information.

1.18 The Contractor shall, as a minimum, have in place robust Business Continuity arrangements and processes including IT disaster recovery plans and procedures that conform to ISO 22301 to ensure that the delivery of the contract is not adversely affected in the event of an incident. An incident shall be defined as any situation that might, or could lead to, a disruption, loss, emergency or crisis to the services delivered. If a ISO 22301 certificate is not available the supplier will provide evidence of the effectiveness of their ISO 22301 conformant Business Continuity arrangements and processes including IT disaster recovery plans and procedures. This should include evidence that the Contractor has tested or exercised these plans within the last 12 months and produced a written report of the outcome, including required actions.

1.19 Any suspected or actual breach of the confidentiality, integrity or availability of Departmental Data being handled in the course of providing this service, or any non-compliance with these Departmental Security Standards for Contractors, or other Security Standards pertaining to the solution, shall be investigated immediately and escalated to the Department by a method agreed by both parties.

1.20 The Contractor shall ensure that any IT systems and hosting environments that are used to handle, store or process Departmental Data shall be subject to independent IT Health Checks (ITHC) using a NCSC approved ITHC provider before go-live and periodically (at least annually) thereafter. The findings of the ITHC relevant to the service being provided are to be shared with the Department and all necessary remedial work carried out. In the event of significant security issues being identified, a follow up remediation test may be required.

1.21 The Contractor or sub-contractors providing the service will provide the Department with full details of any storage of Departmental Data outside of the UK or any future intention to host Departmental Data outside the UK or to perform any form of ICT management, support or development function from outside the UK. The Contractor or sub-contractor will not go ahead with any such proposal without the prior written agreement from the Department.

1.22 The Department reserves the right to audit the Contractor or sub-contractors providing the service within a mutually agreed timeframe but always within seven days of notice of a request to audit being given. The audit shall cover the overall scope of the service being supplied and the Contractor's, and any sub-contractors, compliance with the clauses contained in this Section.

1.23 The Contractor shall contractually enforce all these Departmental Security Standards for Contractors onto any third-party suppliers, sub-contractors or partners who could potentially access Departmental Data in the course of providing this service.

1.24 The Contractor and sub-contractors shall undergo appropriate security assurance activities as determined by the Department. Contractor and sub-contractors shall support the provision of appropriate evidence of assurance and the production of the necessary security documentation such as completing the DfE Security Assurance Model (DSAM) process or the Business Service Assurance Model (BSAM). This will include obtaining any necessary professional security resources required to support the Contractor's and sub-contractor's security assurance activities such as: a NCSC Certified Cyber Security Consultancy (CCSC) or NCSC Certified Professional (CCP) Security and Information Risk Advisor (SIRA).

Schedule 8 – Annex 2

Processing, Personal Data and Data Subjects

The following schedule is the default Department template and both parties will aim to update this via a Change Control Notice by the end of December 2018. In the interim period the Contractor must ensure that they are fully compliant with Data Protection Legislation.

This Schedule 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 Schedule shall be with the Controller at its absolute discretion.

1 The contact details of the Controller's Data Protection Officer is:

[redacted]
Level 1, Sanctuary Buildings, Great Smith Street, London SW1P 3BT
Tel: 020 7783 8656

2 The contact details of the Processor's Data Protection Officer is:

[redacted]
First Floor, Riverside Mill, Mountbatten Way, Congleton, Cheshire, CW12 1DY
Tel: 0330 7260160

3 The Processor shall comply with any further written instructions with respect to processing by the Controller.

4 Any such further instructions shall be incorporated into this Schedule.

Description	Details
Identity of the Controller and Processor	The Parties acknowledge that for the purposes of the Data Protection Legislation, the Customer is the Controller and the Contractor is the Processor in accordance with Clause 17.1.
Subject matter of the processing	[This should be a high level, short description of what the processing is about i.e. its subject matter of the contract. Example: The processing is needed in order to ensure that the Processor can effectively deliver the contract to provide a service to members of the public.]
Duration of the processing	[Clearly set out the duration of the processing including dates]
Nature and purposes of the processing	[Please be as specific as possible, but make sure that you cover all intended purposes. The nature of the processing means any operation such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data (whether or not by automated means) etc. The purpose might include: employment processing, statutory obligation, recruitment assessment etc]
Type of Personal Data	[Examples here include: name, address, date of birth, NI number, telephone number, pay, images, biometric data etc]
Categories of Data Subject	[Examples include: Staff (including volunteers, agents, and temporary workers), Departments/ clients, suppliers, patients, students / pupils, members of the public, users of a particular website etc]

Plan for return and destruction of the data once the processing is complete UNLESS requirement under union or member state law to preserve that type of data	[Describe how long the data will be retained for, how it be returned or destroyed]

Schedule 9 – Commercially Sensitive Information

1.1 Without prejudice to the DFE's general obligation of confidentiality, the Parties acknowledge that the DFE may have to disclose Information in or relating to the Contract following a Request for Information pursuant to clause 16 (Freedom of Information).

1.2 In this Schedule the Parties have sought to identify the Contractor's Confidential Information that is genuinely commercially sensitive and the disclosure of which would be contrary to the public interest.

1.3 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.

1.4 Without prejudice to the DFE's obligation to disclose Information in accordance with the FOIA and the EIR, the DFE will, acting reasonably but in its sole discretion, seek to apply the commercial interests exemption set out in s.43 of the FOIA to the Information listed below.

COMMERCIALLY SENSITIVE INFORMATION	DATE	DURATION OF CONFIDENTIALITY
[redacted]		

Schedule 10 - Financial Distress

1. DEFINITIONS

In this Schedule, the following definitions shall apply:

"Credit Rating Level"	a credit rating level issued by the Rating Agency as specified in Annex 1;
"Credit Rating Threshold"	the minimum Credit Rating Level for the Contractor as set out in Annex 1;
"Rating Agency"	the rating agency listed in Annex 1; and
"Financial Distress Event"	the occurrence of one or more of the events listed in Paragraph 3.1 of this Schedule (*Financial Distress*);
"Financial Distress Service Continuity Plan"	a plan setting out how the Contractor will ensure the continued performance and delivery of the Services in accordance with the Contract in the event that a Financial Distress Event occurs;

2. CREDIT RATING AND DUTY TO NOTIFY

2.1 The Contractor warrants and represents to the DFE for the benefit of the DFE that as at the Commencement Date the Credit Rating Level for the Contractor issued by the Rating Agency is set out in Annex 1.

2.2 The Contractor shall promptly notify (or shall procure that its auditors promptly notify) the DFE in writing if there is any downgrade in the Credit Rating Level issued by the Rating Agency for the Contractor (and in any event within 5 Business Days of the occurrence of the downgrade).

2.3 If there is any downgrade in the Credit Rating Level issued by the Rating Agency for the Contractor, the Contractor shall ensure that the Contractor's auditors thereafter provide the DFE within 10 Business Days of the end of each Year and within 10 Business Days of a written request by the DFE (such requests not to exceed 4 in any Year) with written calculations of the quick ratio for the Contractor as at the end of each Year or such other date as may be requested by the DFE. For these purposes the "quick ratio" on any date means:

$$\frac{A+B+C}{D}$$

where:

(a) is the value at the relevant date of all cash in hand and at the bank of the Contractor;

(b) is the value of all marketable securities held by the Contractor determined using closing prices on the Business Day preceding the relevant date;

(c) is the value at the relevant date of all account receivables of the Contractor; and

(d) is the value at the relevant date of the current liabilities of the Contractor.

2. The Contractor shall:

(a) regularly monitor the Credit Rating Level of the Contractor with the Rating Agency; and

(b) promptly notify (or shall procure that its auditors promptly notify) the DFE in writing following the occurrence of a Financial Distress Event or any fact, circumstance or matter which could cause a Financial Distress Event and in any event, ensure that such notification is made within 10 Business Days of the date on which the Contractor first becomes aware of the Financial Distress Event or the fact, circumstance or matter which could cause a Financial Distress Event.

2.5 For the purposes of determining whether a Financial Distress Event has occurred pursuant to the provisions of Paragraph 3.1(a), the credit rating of the Contractor, shall be deemed to have dropped below the Credit Rating Threshold if the Rating Agency has rated the Contractor at or below the Credit Rating Threshold.

3. CONSEQUENCES OF A FINANCIAL DISTRESS EVENT

3.1 The following shall constitute a Financial Distress Event:

(a) the Credit Rating Level of the Contractor dropping below the Credit Rating Threshold;

(b) the Contractor issuing a profits warning to a stock exchange or making any other public announcement, in each case about a material deterioration in its financial position or prospects;

(c) there being a public investigation into improper financial accounting and reporting, suspected fraud or any other impropriety of the Contractor;

(d) the Contractor committing a material breach of covenant to its lenders;

(e) a Sub-contractor notifying the DFE that the Contractor has not satisfied any material sums properly due under a specified invoice and not subject to a genuine dispute; or

(f) any of the following:

i) commencement of any litigation against the Contractor with respect to financial indebtedness

ii) non-payment by the Contractor of any financial indebtedness;

iii) any financial indebtedness of the Contractor becoming due as a result of an event of default; or

iv) the cancellation or suspension of any financial indebtedness in respect of the Contractor,

in each case which the DFE reasonably believes (or would be likely reasonably to believe) could directly impact on the continued performance and delivery of the Services in accordance with this Contract;

3.2 Immediately upon notification of the Financial Distress Event to the DFE by the Contractor (or if the DFE becomes aware of the Financial Distress Event without notification and bring the event to the attention of the Contractor), the Contractor shall have the obligations and the DFE shall have the rights and remedies set out in paragraphs 3.3 to 3.6.

3.3 In the event of a late or non-payment of a Sub-contractor pursuant to Paragraph 3.1(f), the DFE shall not exercise any of its rights or remedies under Paragraph 3.4 without first giving the Contractor 10 Business Days to:

(a) rectify such late or non-payment; or

(b) demonstrate to the DFE's reasonable satisfaction that there is a valid reason for late or non-payment.

3.4 The Contractor shall:

(a) at the request of the DFE, meet the DFE as soon as reasonably practicable (and in any event within 3 Business Days of the initial notification (or awareness) of the Financial Distress Event (or such other period as the DFE may permit and notify to the Contractor in writing) to review the effect of the Financial Distress Event on the continued performance and delivery of the Services in accordance with this Contract; and

(b) where the DFE reasonably believes (taking into account the discussions and any representations made under Paragraph 3.4 (a) that the Financial Distress Event could impact on the continued performance and delivery of the Services in accordance with this Contract:

i) submit to the DFE for its approval, a draft Financial Distress Service Continuity Plan as soon as reasonably practicable (and in any event, within 10 Business Days of the initial notification (or awareness) of the Financial Distress Event or such other period as the DFE may permit and notify to the Contractor in writing); and

(c) provide such financial information relating to the Contractor as the DFE may reasonably require.

3.5 The DFE shall not withhold its approval of a draft Financial Distress Service Continuity Plan unreasonably. If the DFE does not approve the draft Financial Distress Service Continuity Plan, it shall inform the Contractor of its reasons and the Contractor shall take those reasons into account in the preparation of a further draft Financial Distress Service Continuity Plan, which shall be resubmitted to the DFE within 5 Business Days of the rejection of the first draft. This process shall be repeated until the Financial Distress Service Continuity Plan is approved by DFE or referred to the Dispute Resolution Procedure under Paragraph 3.6.

3.6 If the DFE considers that the draft Financial Distress Service Continuity Plan is insufficiently detailed to be properly evaluated, will take too long to complete or will not ensure the continued performance of the Contractor's obligations in accordance with the Contract, then it may either agree a further time period for the development and agreement of the Financial Distress Service Continuity Plan or escalate any issues with the draft Financial Distress Service Continuity Plan using the Dispute Resolution Procedure.

3.7 Following approval of the Financial Distress Service Continuity Plan by the DFE, the Contractor shall:

(a) on a regular basis (which shall not be less than monthly), review the Financial Distress Service Continuity Plan and assess whether it remains adequate and up to date to ensure the continued performance and delivery of the Services in accordance with this Contract;

(b) where the Financial Distress Service Continuity Plan is not adequate or up to date in accordance with Paragraph 3.7(a), submit an updated Financial Distress Service Continuity Plan to the DFE for its approval, and the provisions of Paragraphs 3.5 and 3.6 shall apply to the review and approval process for the updated Financial Distress Service Continuity Plan; and

(c) comply with the Financial Distress Service Continuity Plan (including any updated Financial Distress Service Continuity Plan).

3.8 Where the Contractor reasonably believes that the relevant Financial Distress Event under Paragraph 3.1 (or the circumstance or matter which has caused or otherwise led to it) no longer exists, it shall notify the DFE and the Parties may agree that the Contractor shall be relieved of its obligations under Paragraph 3.7.

4. TERMINATION RIGHTS

4.1 The DFE shall be entitled to terminate this Contract if:

(a) the Contractor fails to notify the DFE of a Financial Distress Event in accordance with Paragraph 2.4(b).

(b) the Parties fail to agree a Financial Distress Service Continuity Plan (or any updated Financial Distress Service Continuity Plan) in accordance with Paragraphs 3.4 to 3.6; and/or

(c) the Contractor fails to comply with the terms of the Financial Distress Service Continuity Plan (or any updated Financial Distress Service Continuity Plan) in accordance with Paragraph 3.7(c).

5. PRIMACY OF CREDIT RATINGS

5.1 Without prejudice to the Contractor's obligations and the DFE's rights and remedies under Paragraph 2, if, following the occurrence of a Financial Distress Event pursuant to any of Paragraphs 3.1(b) to 3.1(f), the Rating Agencies review and report subsequently that the credit ratings do not drop below the relevant Credit Rating Threshold, then:

(a) the Contractor shall be relieved automatically of its obligations under Paragraphs 3.4; and

(b) the DFE shall not be entitled to require the Contractor to provide financial information in accordance with Paragraph 3.4(c).

Schedule 10 – Annex 1

Rating Agency

Supplier Registration (Sid4Gov)

Credit Rating Level

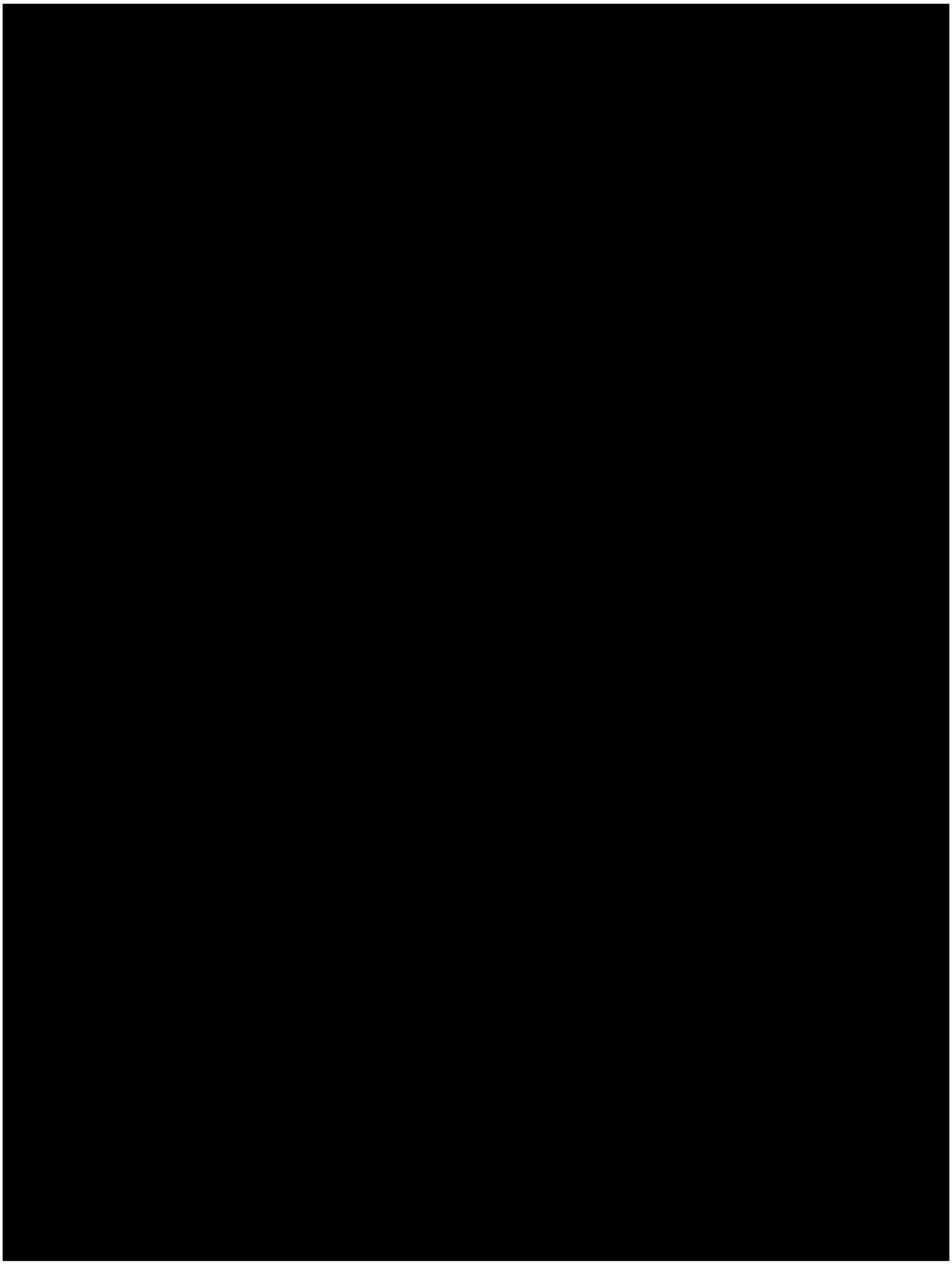
[redacted]

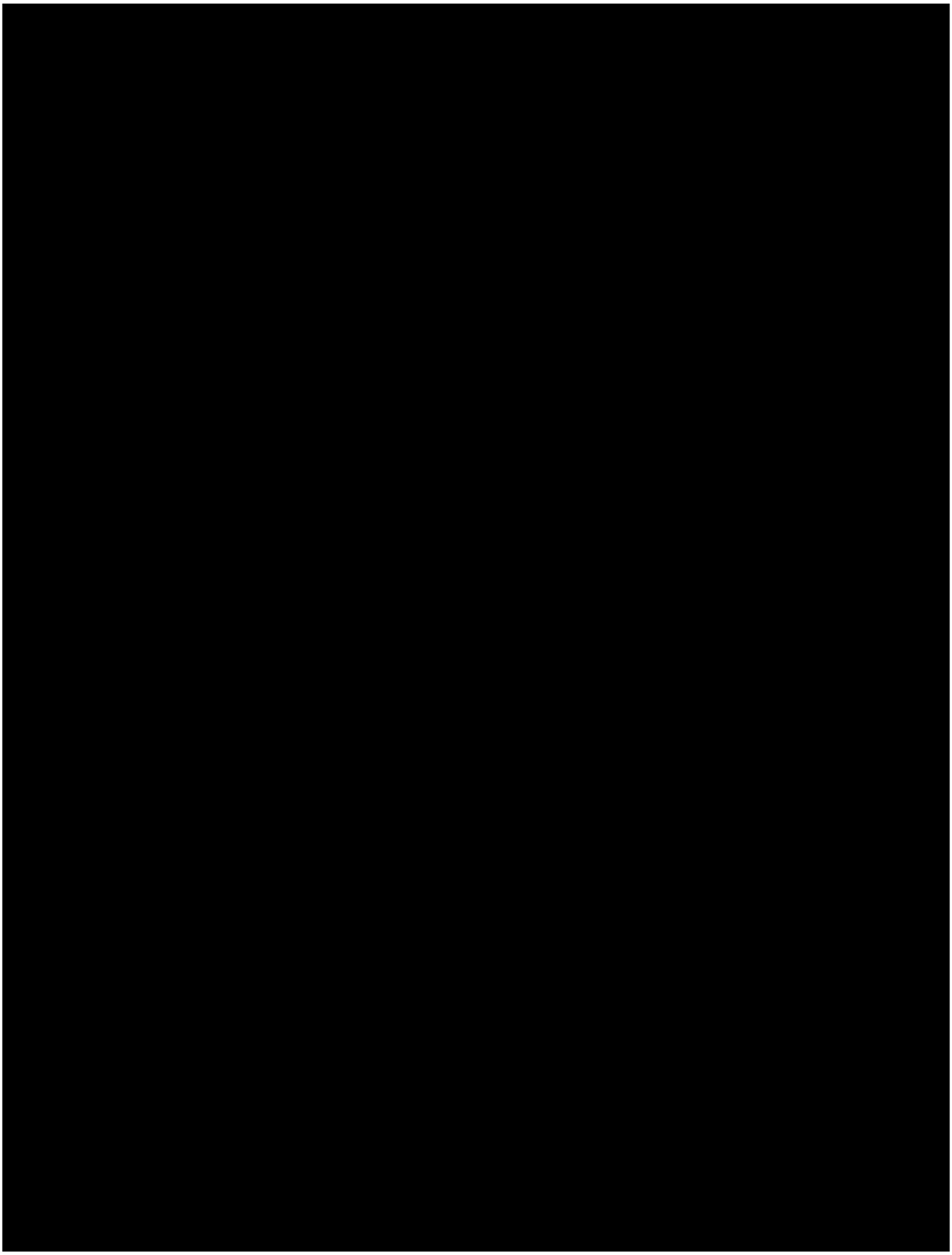
- Rating Agency 1: Supplier Registration (Sid4Gov)

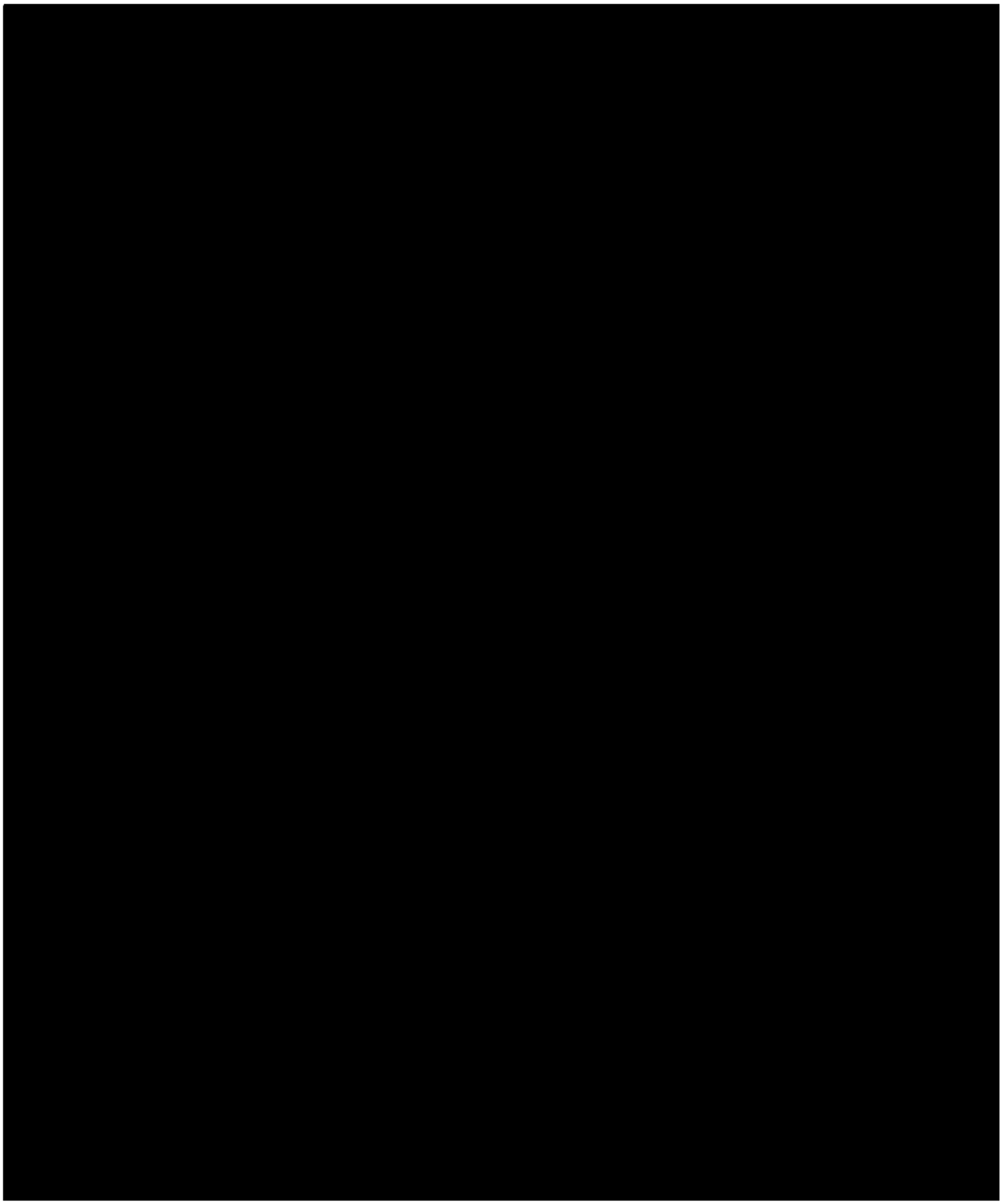
Credit Rating Threshold

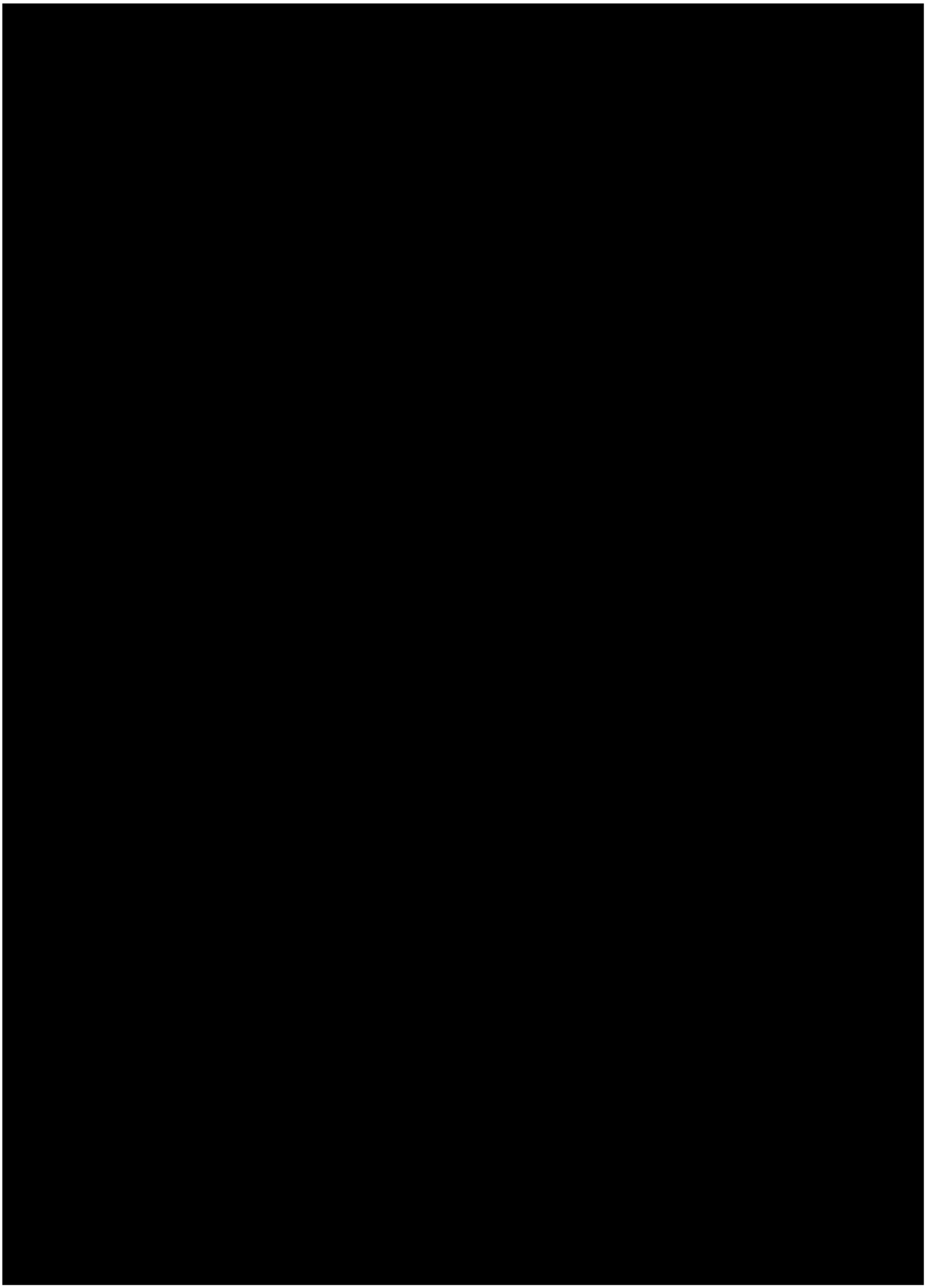
Entity	Credit Rating	Credit Threshold
[redacted]		

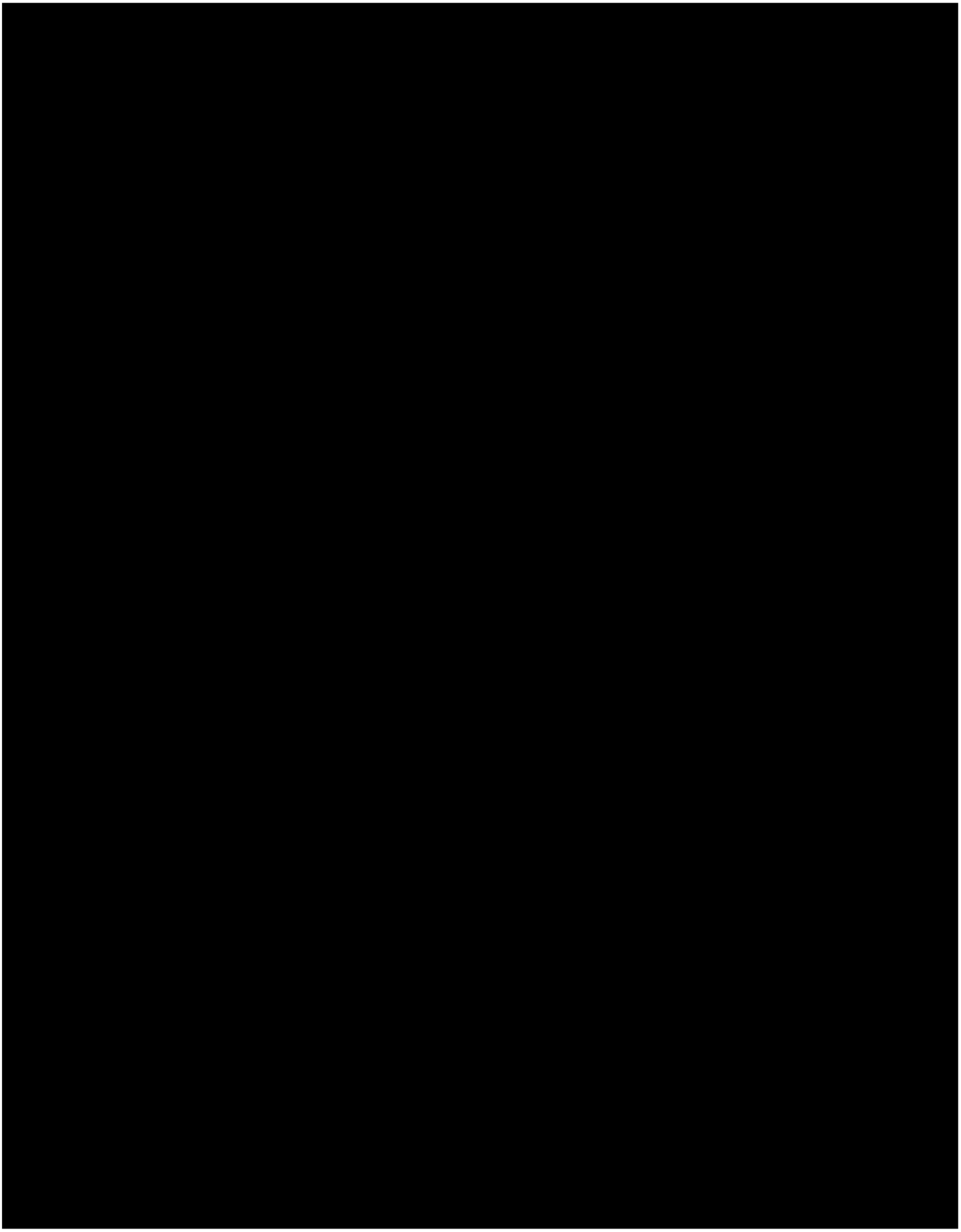
Schedule 11 – The Contractor's Solution



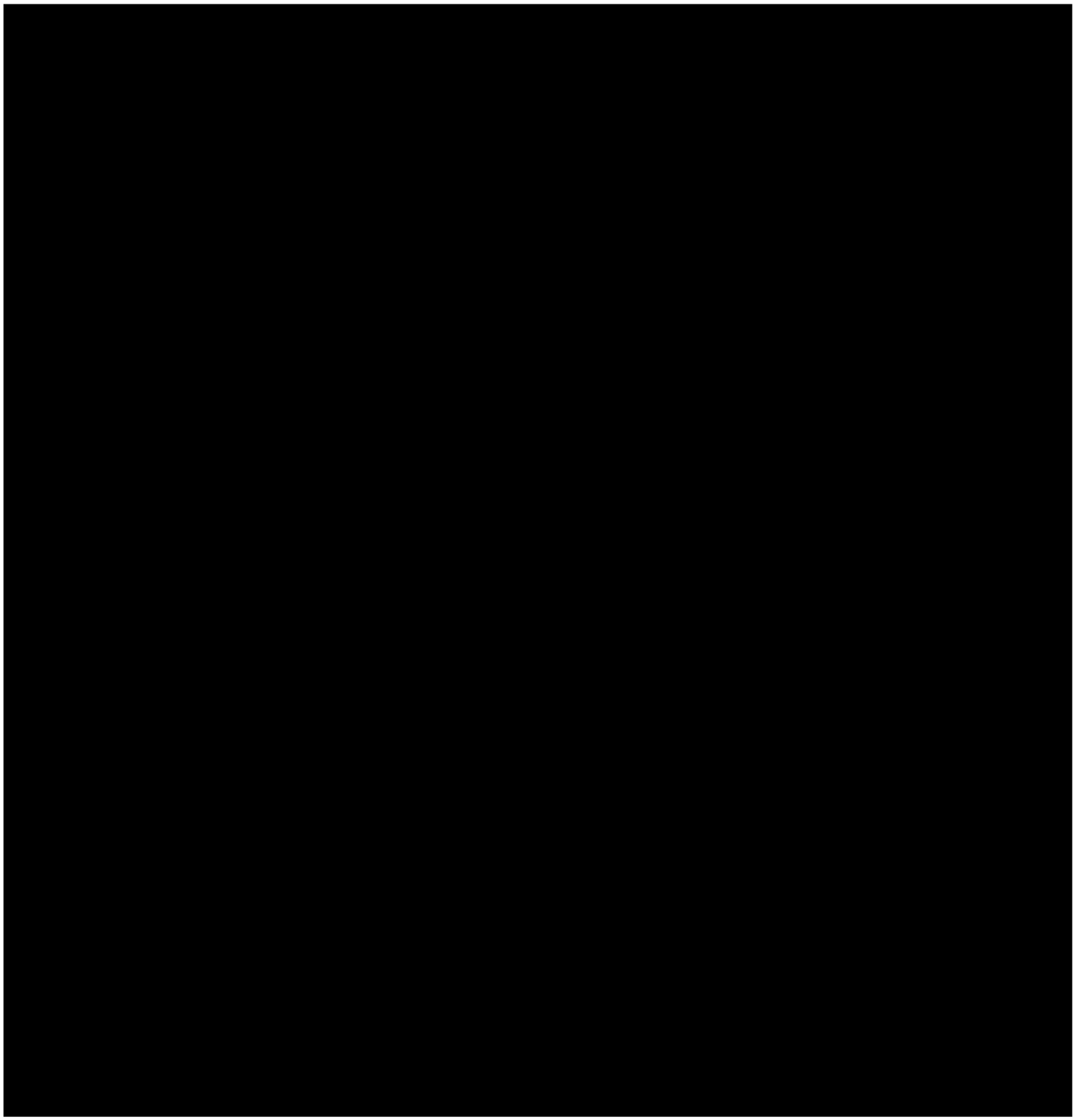


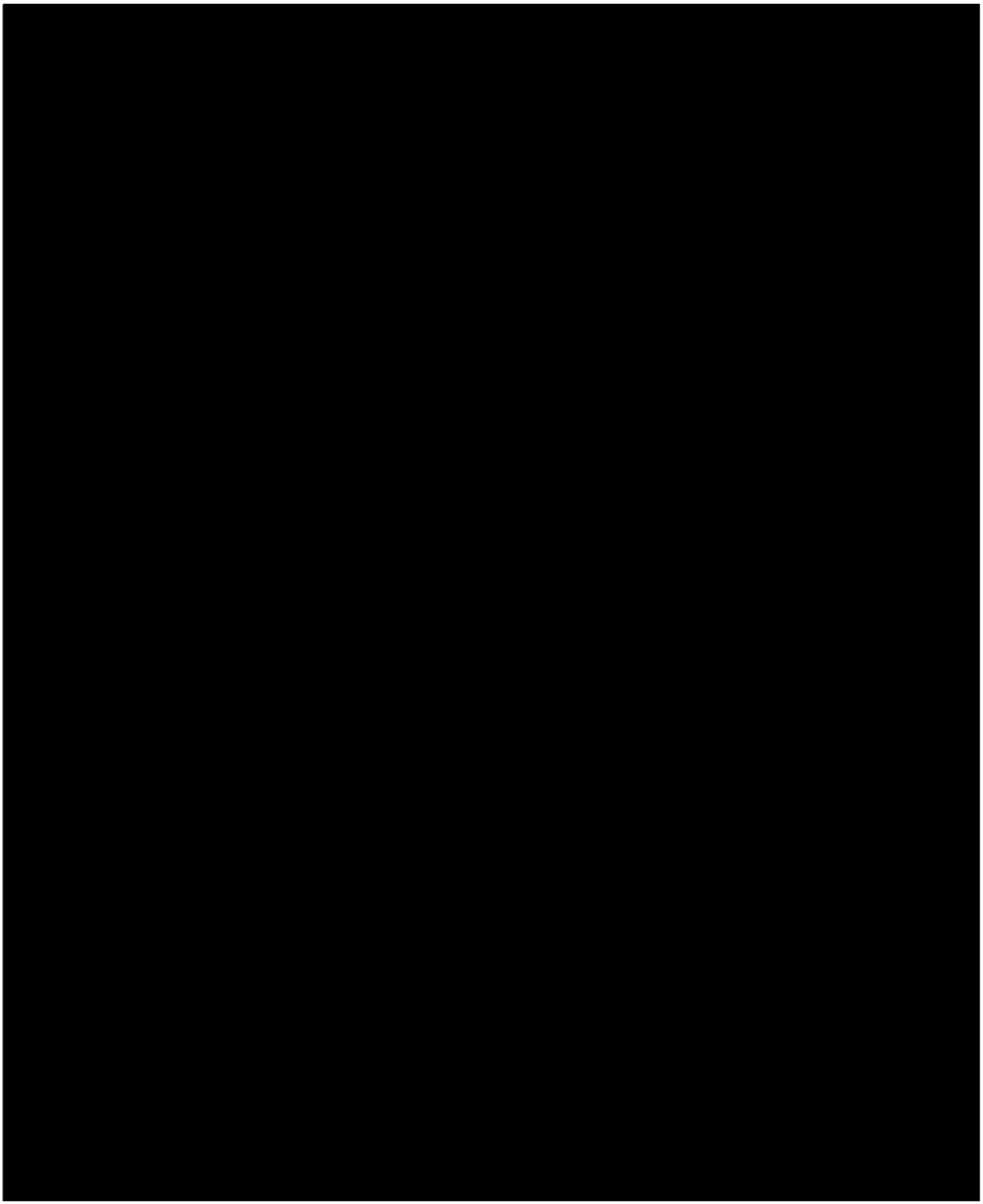


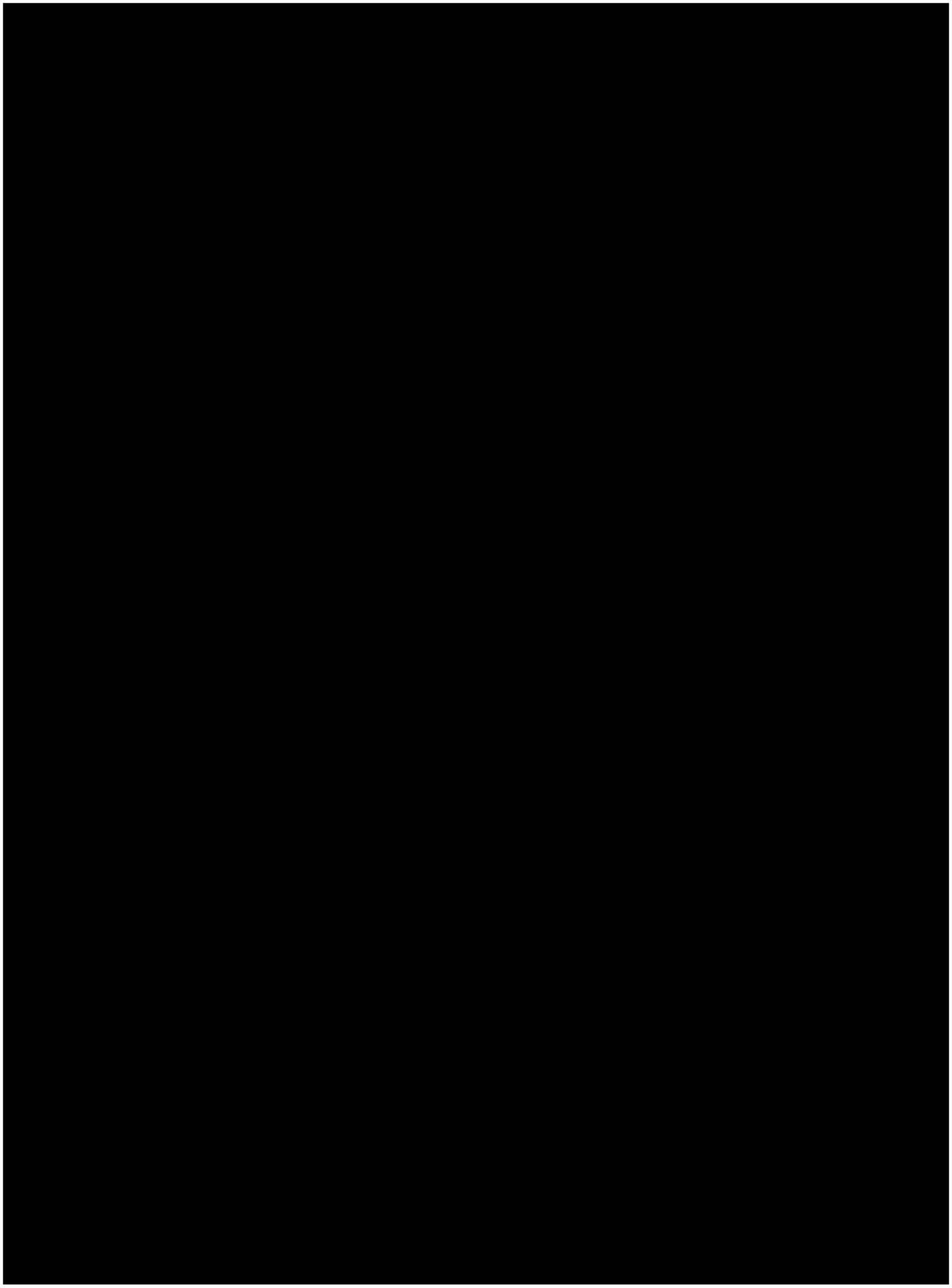


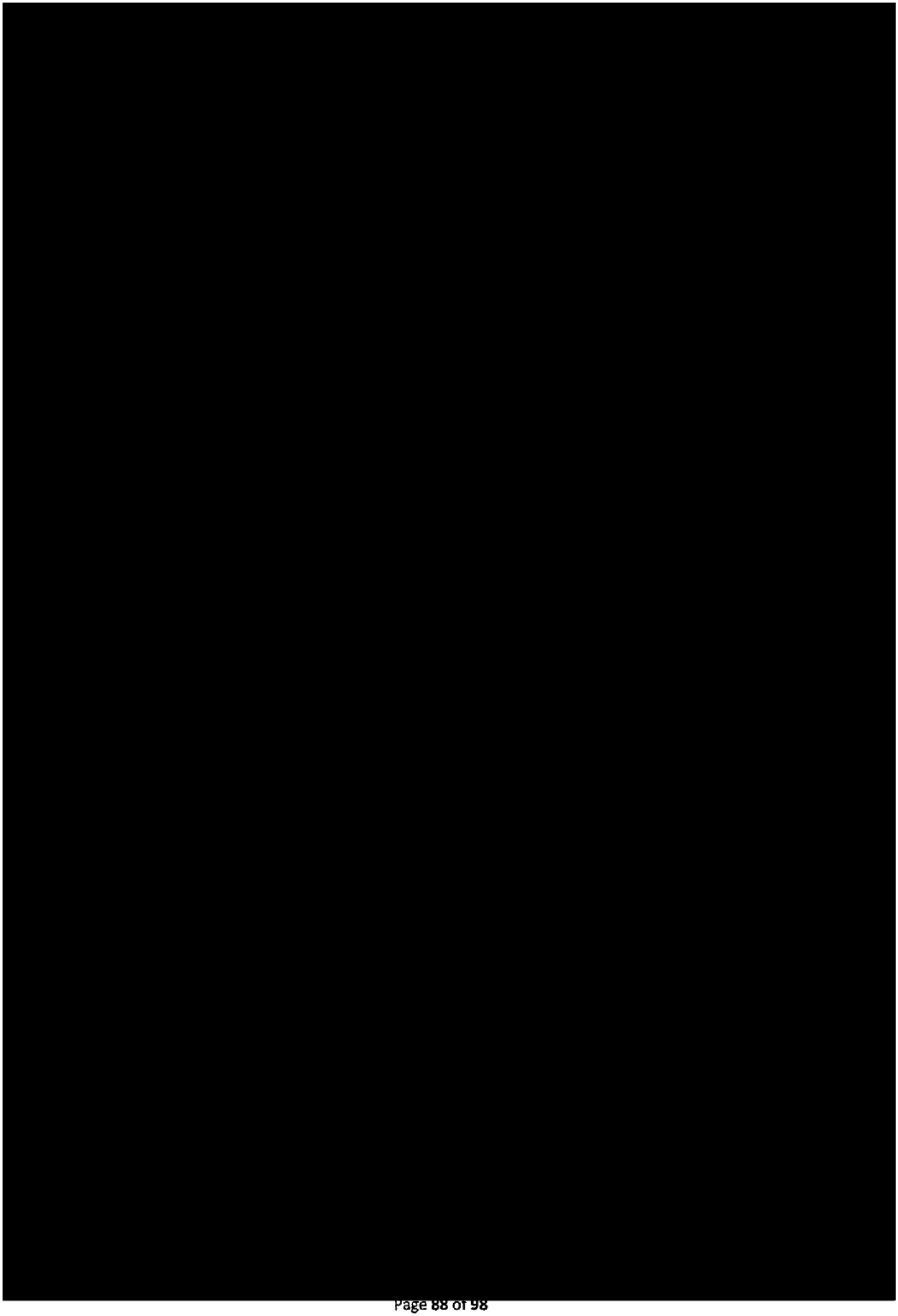


[redacted]









[redacted]