

**North Carolina Department of
Health and Human Services
Division of Child Development
and Early Education**

RFP #30-23189

**Workforce Registry and NC Pre-K and
Regulatory System Replacement**

**North Carolina Department of Health and Human Services,
Division of Child Development and Early Education**

Workforce Registry and NC Pre-K and Regulatory System Replacement

RFP #30-23189

August 17, 2023

Submitted to:

NCDHHS - Division of Child Development and
Early Education

Maureen Salman

Contracting Specialist

Email address: maureen.salman@dhhs.nc.gov

Submitted by:

Accenture

Natalie Batten

Managing Director

Phone number: 919-247-5228

Email address: natalie.batten@accenture.com

a) Signed Execution Page

STATE OF NORTH CAROLINA Department of Health and Human Services	REQUEST FOR PROPOSAL NO. 30-23189
	Offers will be publicly opened:
Refer <u>ALL</u> inquiries regarding this RFP to: Maureen Salman Contract Specialist Office of Procurements, Contracts and Grants maureen.salman@dhhs.nc.gov	Issue Date: June 27, 2023
	Commodity Number: 811118
	Description: DCDEE - Workforce Registry and NC Pre-K and Regulatory System Replacement
	Purchasing Agency: Department of Health and Human Services (DHHS), Division of Child Development and Early Education (DCDEE)
	Requisition No.: <input type="text"/>

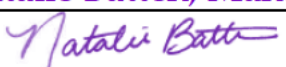
OFFER

The Purchasing Agency solicits offers for Services and/or goods described in this solicitation. All offers and responses received shall be treated as Offers to contract as defined in 9 NCAC 06A.0102(12).

EXECUTION

In compliance with this Request for Proposal, and subject to all the conditions herein, the undersigned offers and agrees to furnish any or all Services or goods upon which prices are offered, at the price(s) offered herein, within the time specified herein.

Failure to execute/sign offer prior to submittal shall render offer invalid. Late offers are not acceptable.

OFFEROR: Accenture LLP			
STREET ADDRESS: 555 Fayetteville Street, Unit 820		P.O. BOX:	ZIP: 27601
CITY, STATE & ZIP: Raleigh, NC, 27601		TELEPHONE NUMBER: 919-247-5228	TOLL FREE TEL. NO
PRINT NAME & TITLE OF PERSON SIGNING: Natalie Batten, Managing Director		FAX NUMBER:	
AUTHORIZED SIGNATURE: 	DATE: 8/17/2023	E-MAIL: natalie.batten@accenture.com	

Offer valid for ninety (90) days from date of offer opening unless otherwise stated here: days

ACCEPTANCE OF OFFER

If any or all parts of this offer are accepted, an authorized representative of DCDEE shall affix its signature hereto and any subsequent Request for Best and Final Offer, if issued. Acceptance shall create a contract having an order of precedence as follows: Best and Final Offers, if any, Special terms and conditions specific to this RFP, Specifications of the RFP, the Department of Information Technology Terms and Conditions, Department of Health and Human Services Terms and Conditions, and the agreed portion of the awarded Vendor's Offer. A copy of this acceptance will be forwarded to the awarded Vendor(s).

<u>FOR PURCHASING AGENCY USE ONLY</u>	
Offer accepted and contract awarded this date by	, as indicated on attached certification, (Authorized representative of Purchasing Agency Name).

August 17, 2023

Solicitation Number: RFP# 30-23189

NC Department of Health and Human Services - Division of Child Development and Early Education

Attn: Maureen Salman - Contracting Specialist

Dear Mrs. Salman:

Accenture LLP ("Accenture") is honored to submit our proposal in response to the Department of Health and Human Services RFP # 30-23189. As requested, this response is valid for a period of ninety (90) days from the date of offer opening. We are eager for the chance to apply our expertise in modernizing the business processes of the Child Care Regulatory System.

As the submitting organization, Accenture brings the Division of Child Development and Early Education (DCDEE) our deep understanding of NCDHHS, regulatory and compliance, and early childhood education, in addition to our implementation expertise necessary to provide an advanced solution. This solution is set to not only optimize the processing and reporting of data, automate manual processes, and amplify program operations within your desired timeframe, but also offer DCDEE a system that will bolster the future growth of the Child Care Regulatory System.

We are fully invested in DCDEE's journey and value this opportunity to continue our long-term, successful partnership with you. We are proud to bring:

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

As the Client Account Lead for Accenture's work with the State of North Carolina, I am authorized to obligate Accenture related to this RFP, negotiate on behalf of our organization. Furthermore, I am your primary contact for any required clarifications. You'll find my contact information below my signature. We acknowledge receipt of all amendments to the RFP (2 in total).

As NCDHHS seeks to equip the Child Care Regulatory System with a cutting-edge platform, we are thrilled to present our approach and capabilities to turn your vision into reality. We look forward to introducing you to the team and reviewing our proposal in detail with you.

Sincerely,



Managing Director, Accenture

State of North Carolina Client Account Lead

Raleigh, North Carolina | Phone: 919-247-5228 | Email: natalie.batten@accenture.com

b) Table of Contents

a) Execution Page	A - 1
b) Table of Contents	B - 1
Executive Summary	Ex - 1
c) Description of Vendor Submitting Offer (Attachment D)	C - 1
d) Vendor Response to Specifications and Requirements	D - 1
3.1 General Requirements and Specifications	D - 4
3.2 Security Requirements and Specifications	D - 6
3.3 Enterprise Specifications	D - 6
3.4 Business and Technical Specifications	D - 8
3.5 Management Specifications	D - 106
e) Security Vendor Readiness Assessment Report (VRAR)	E - 1
f) Architecture Diagrams	F - 1
g) Cost Form for Vendor's Offer (Attachment E)	G - 1
h) Schedule of Offered Solution.....	H - 1
i) Signed Vendor Certification Form (Attachment F)	i - 1
j) Location of Workers Utilized by Agency (Attachment G)	J - 1
k) References	K - 1
l) Financial Statements (Attachment I)	L - 1
m) Errata and Exceptions, if any.....	M - 1
n) Vendor's License and Maintenance Agreements, if any, and Third-Party License Agreements, if any	N - 1
o) Supporting material such as technical system documentation, training examples, etc.....	O - 1
p) Vendor may attach other supporting materials that it feels may improve the quality of its response. These materials should be included as items in a separate appendix.	P - 1
q) All Pages of the Solicitation (including Attachments A, B, and C).....	Q - 1
r) Draft Plans	R - 1
1.0 Draft Vendor Project Management Plan	R - 4
2.0 Draft Vendor Project Schedule	R - 43
3.0 Draft Vendor Staffing Plan	R - 44
4.0 Draft Service Level Agreement.....	R - 72
5.0 Draft Vendor Operations and Maintenance Phase Staffing Plan.....	R - 97

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

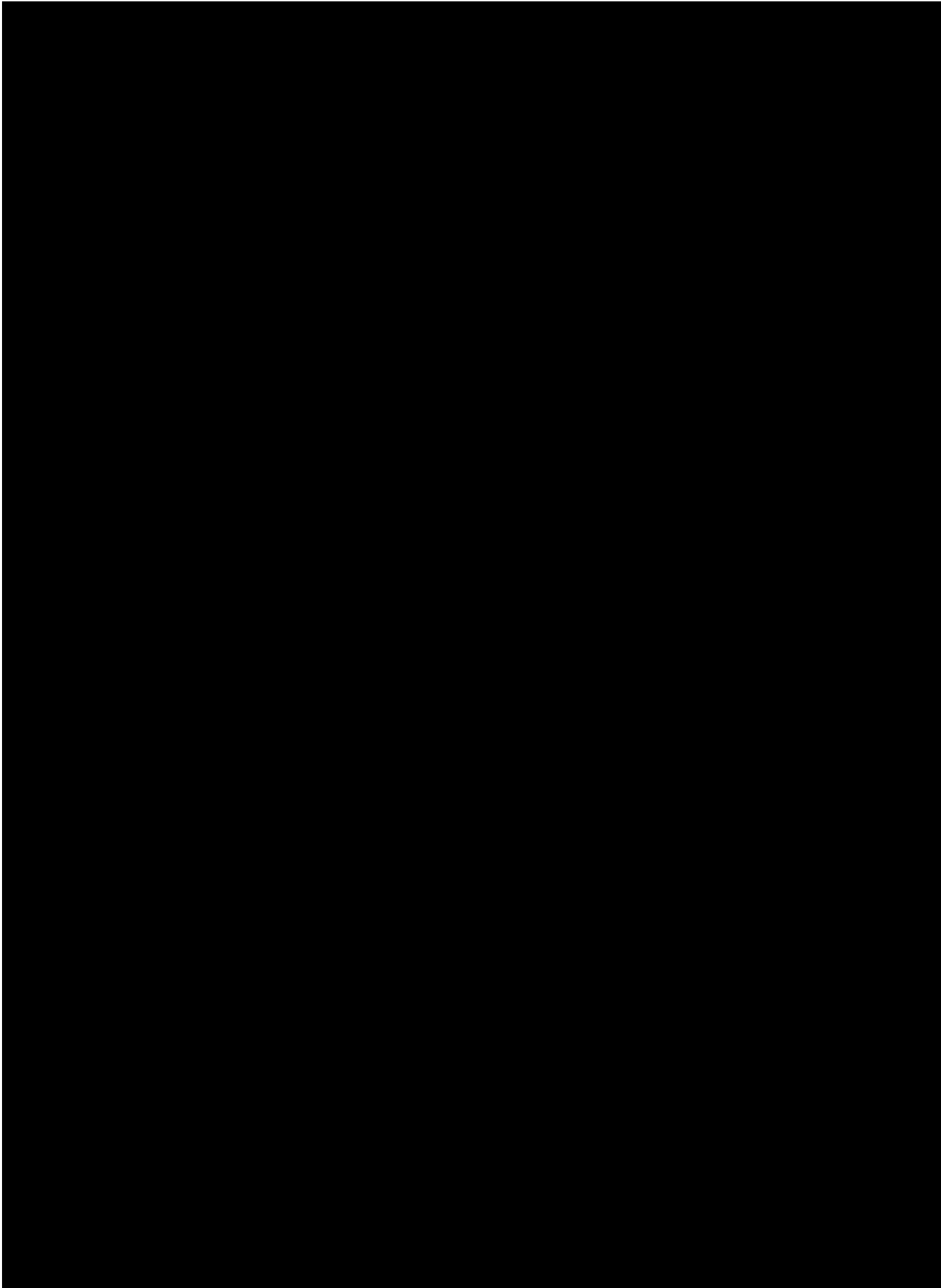


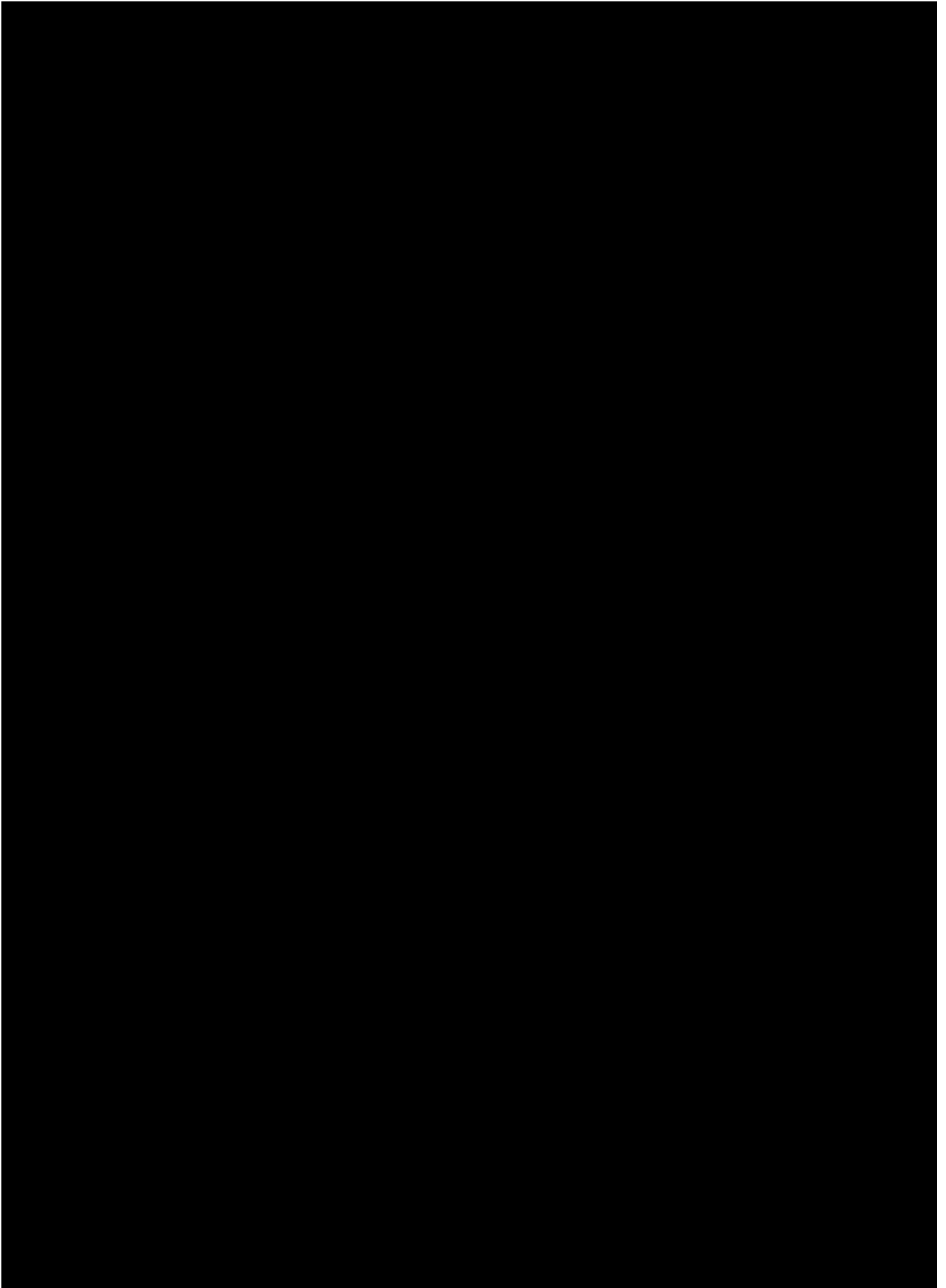
[REDACTED]

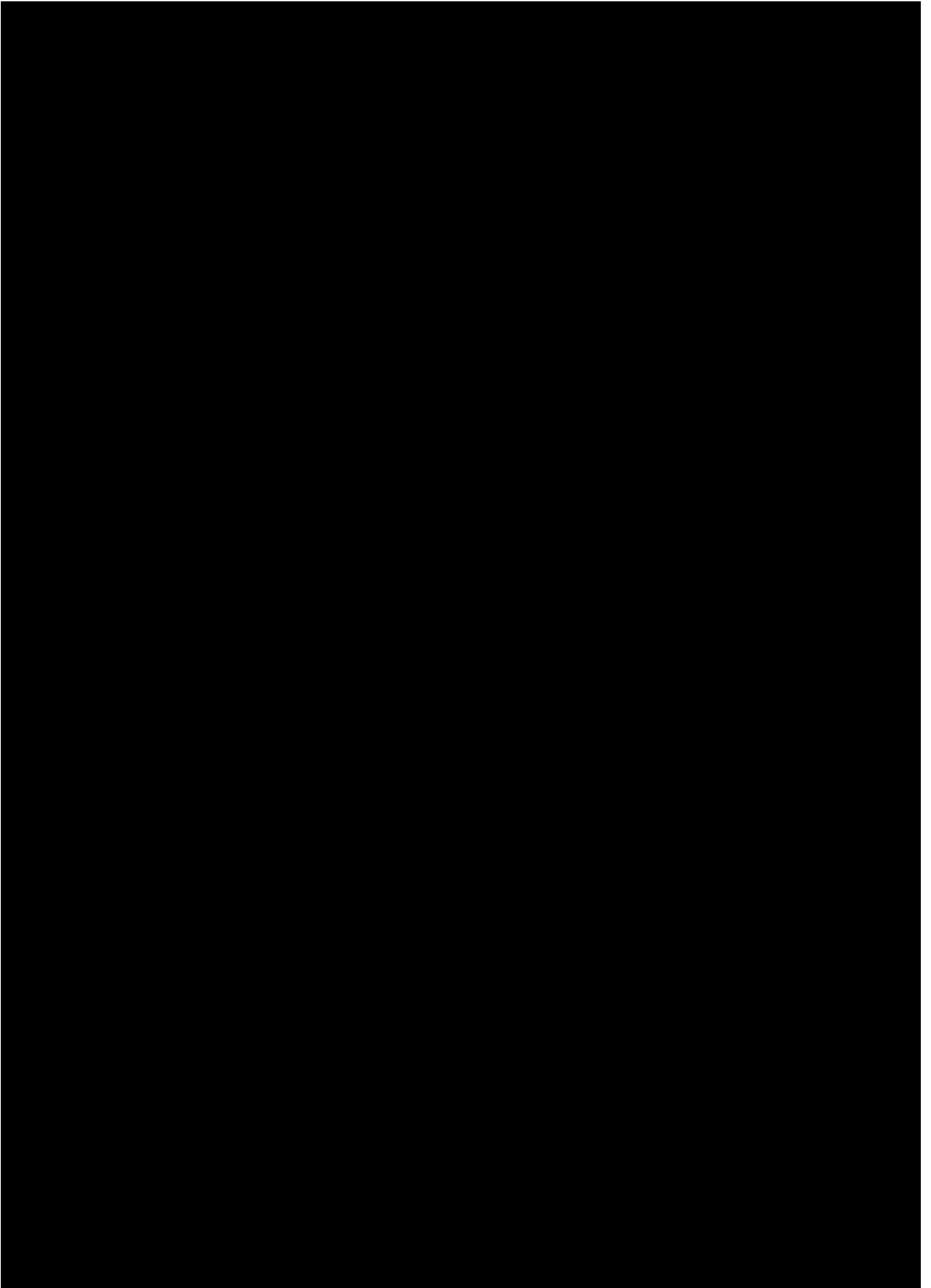
[REDACTED]

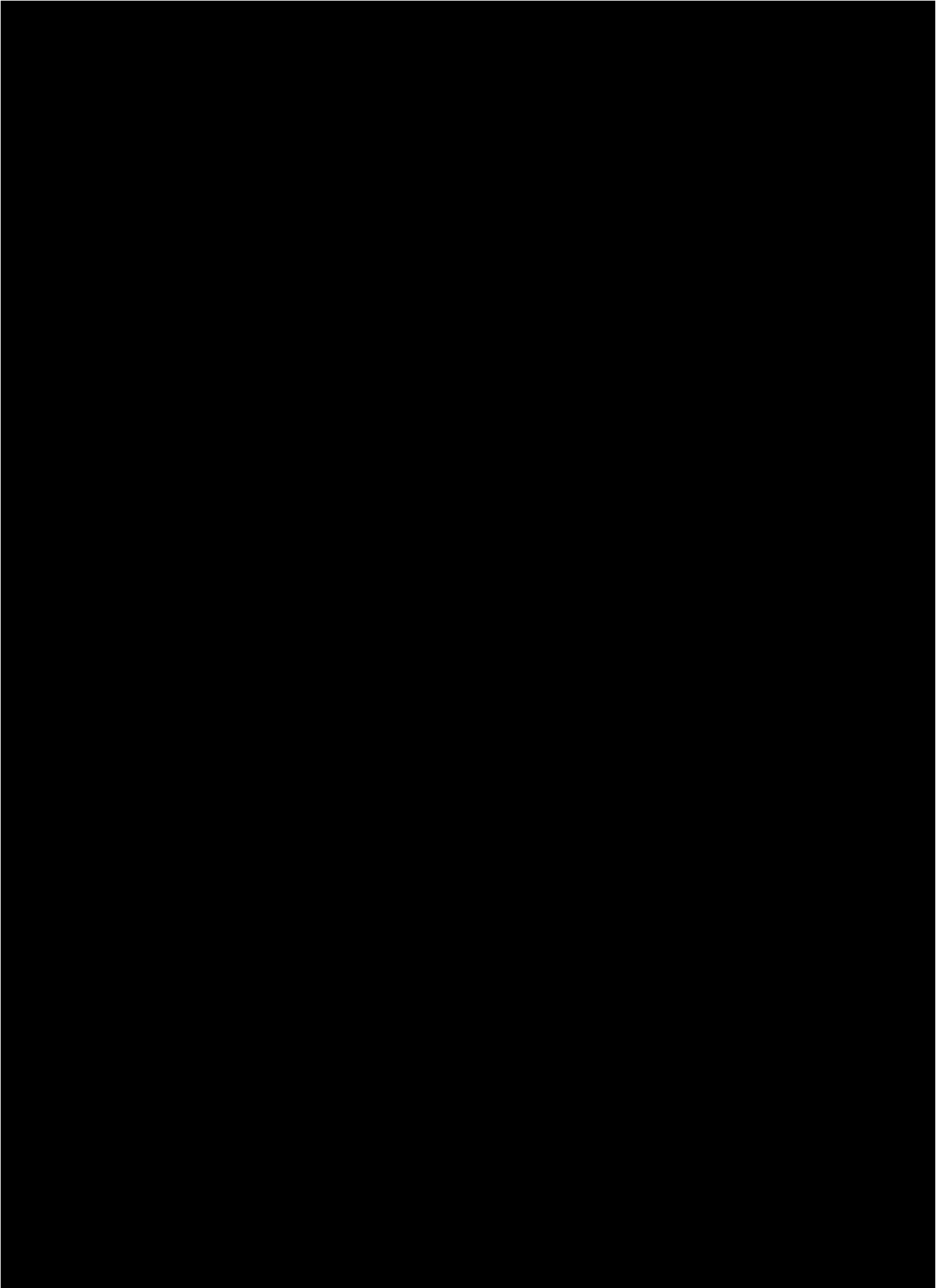
[REDACTED]

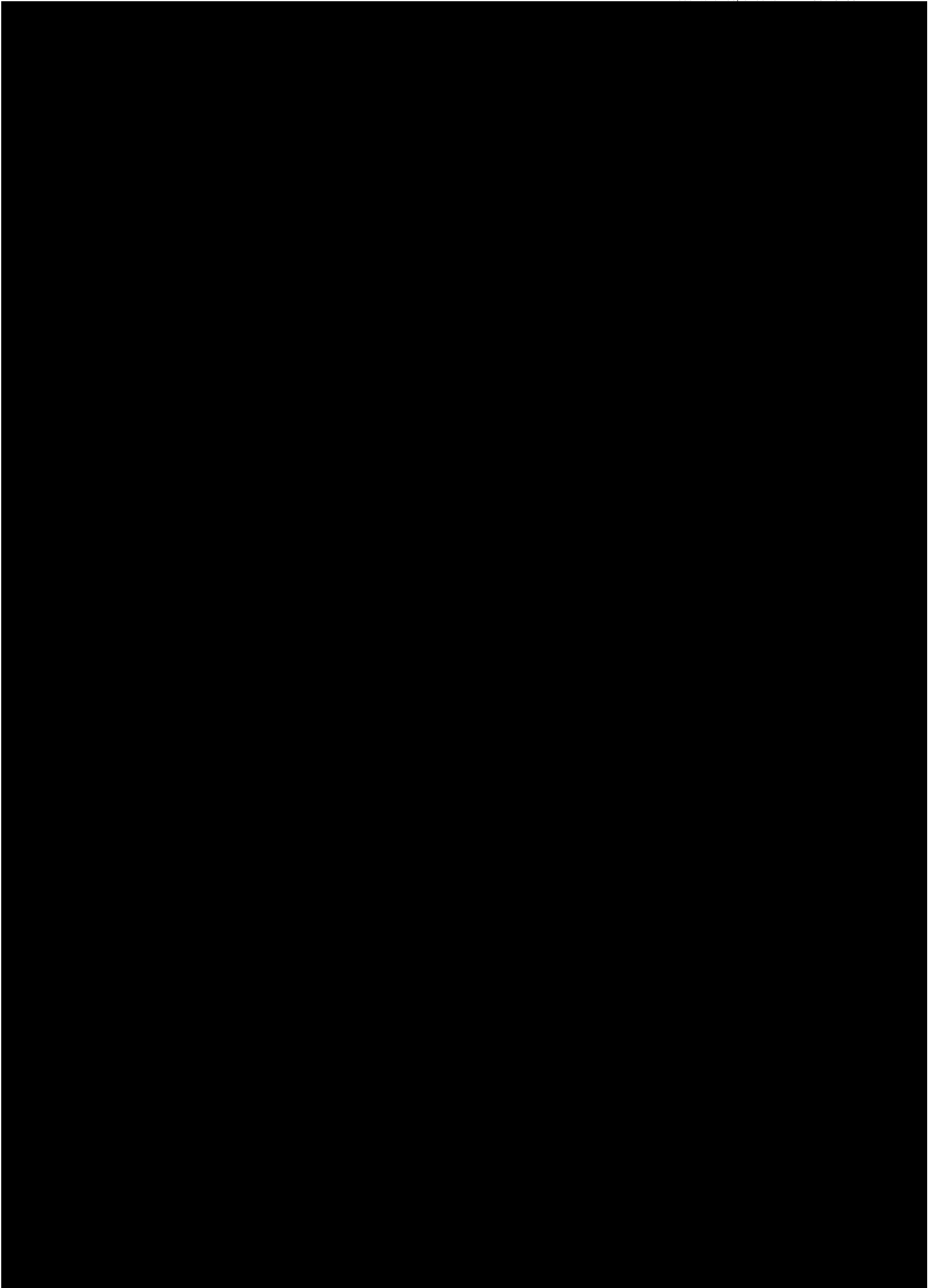
[REDACTED]

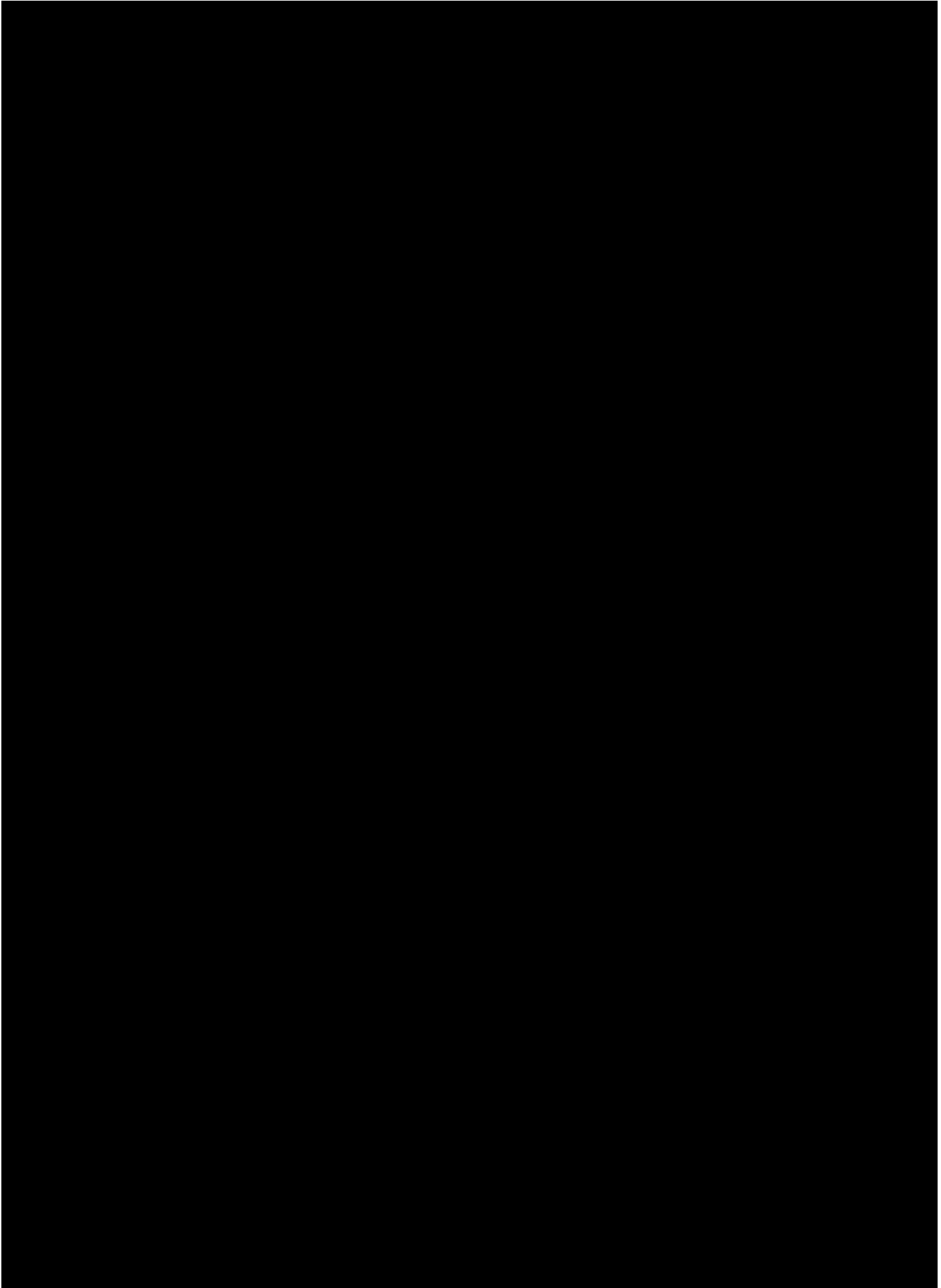


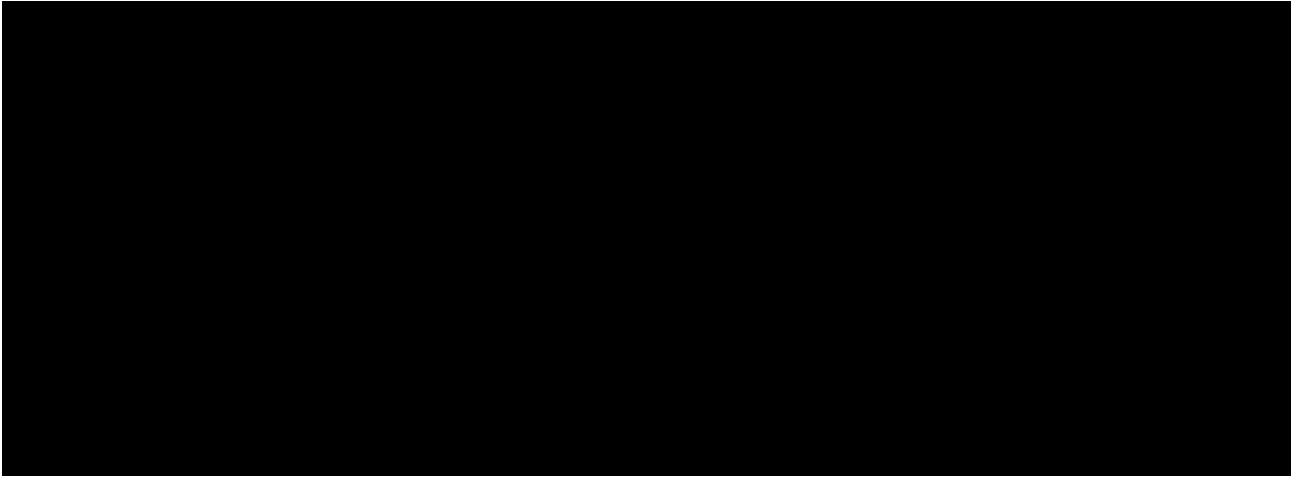














Section c)

Description of Vendor Submitting Offer

c) Description of Vendor Submitting Offer Form

ATTACHMENT D: DESCRIPTION OF OFFEROR
Provide the information about the offeror.

Offeror's full name	Accenture LLP
Offeror's address	Raleigh, NC 555 Fayetteville Street, Suite 820 Raleigh, NC 27601 Principal Office 500 W Madison St Chicago, IL 60661
Offeror's telephone number	919-836-1200
Ownership	<input checked="" type="checkbox"/> Public <input type="checkbox"/> Partnership <input type="checkbox"/> Subsidiary <input type="checkbox"/> Other (specify)
Date established	Accenture was founded in 1989 Date formed on NC business registry: 3/11/2002
If incorporated, state of incorporation.	Illinois
North Carolina Secretary of State Registration Number, if currently registered	0623314
Number of full-time employees on January 1st for the last three years or for the duration that the Vendor has been in business, whichever is less.	738,000 as of January 1, 2023 674,000 as of January 1, 2022 537,000 as of January 1, 2021 Accenture's most recent count of full-time employees is published on Accenture's website: https://www.accenture.com/us-en/about/company-index
Offeror's Contact for Clarification of Offer: Contact's name Title Email address and Telephone number	Angela Harwanko Managing Director State of North Carolina Technology Services Lead angela.w.harwanko@accenture.com / 703-966-3344
Offeror's Contact for Negotiation of offer: Contact's name Title Email address and Telephone Number	Natalie Batten Managing Director State of North Carolina Client Account Lead natalie.batten@accenture.com / 919-247-5228

If Contract is Awarded, Offeror's Contact for Contractual Issues:	
Contact's name	Natalie Batten
Title	Managing Director
Email address and Telephone Number	State of North Carolina Client Account Lead natalie.batten@accenture.com / 919-247-5228
If Contract is Awarded, Offeror's Contact for Technical Issues:	
Contact's name	Natalie Batten
Title	Managing Director
Email address and Telephone Number	State of North Carolina Client Account Lead natalie.batten@accenture.com / 919-247-5228

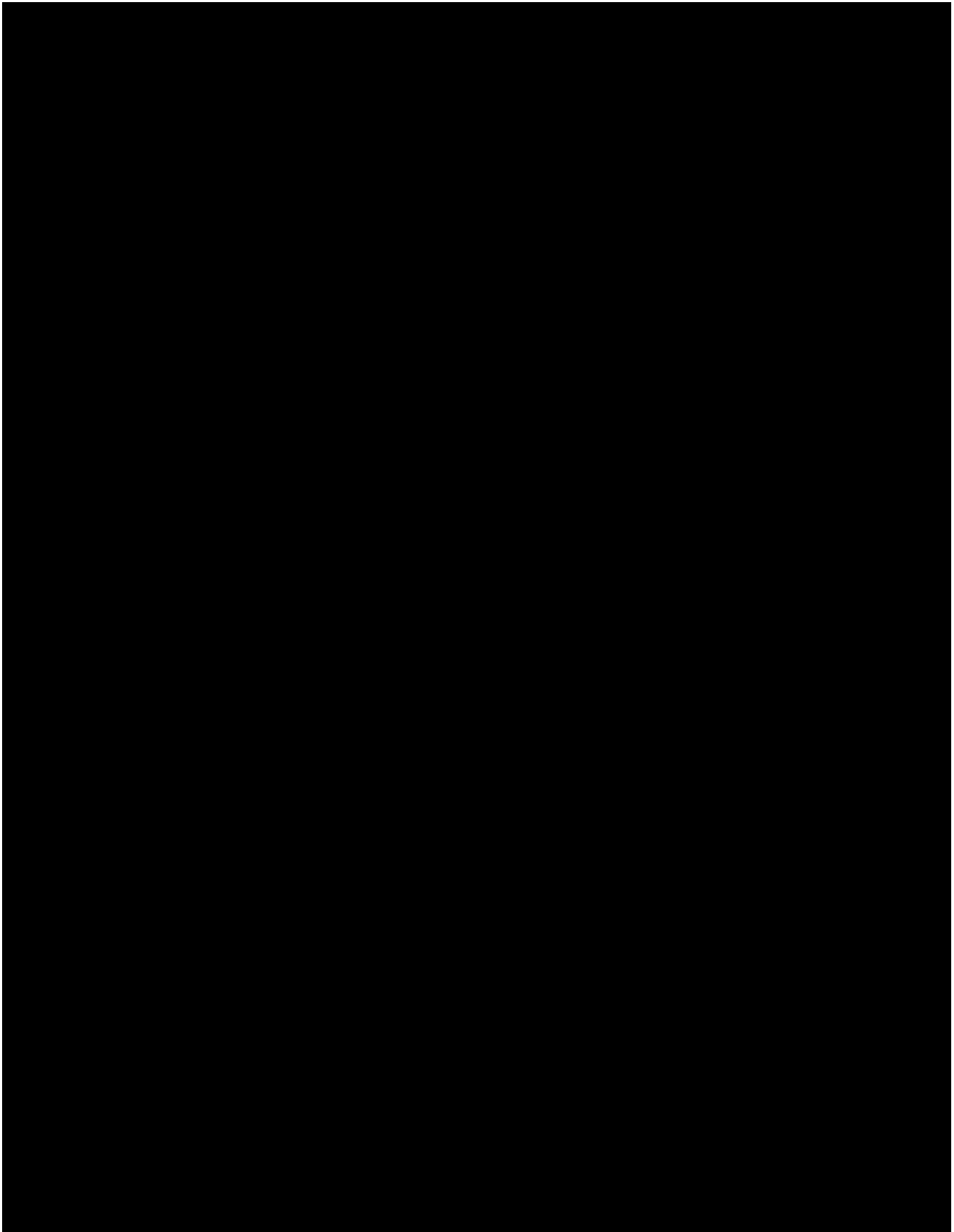


Section d)

Vendor Response to Specifications and Requirements

d) Vendor Response to Specifications and Requirements





3.1 General Requirements and Specifications

3.1.1 Requirements

Means, as used herein, a function, feature, or performance that the system must provide. See subsequent sections for requirements.

No response required.

3.1.2 Specifications

Means, as used herein, a specification that documents the function and performance of a system or system component. The apparent silence of the specifications as to any detail, or the apparent omission of detailed description concerning any point, shall be regarded as meaning that only the best commercial practice is to prevail and that only processes, configurations, materials and workmanship of the first quality may be used. Upon any notice of noncompliance provided by the State, Vendor shall supply proof of compliance with the specifications. Vendor must provide written notice of its intent to deliver alternate or substitute Services, products, goods or other Deliverables. Alternate or substitute Services, products, goods or Deliverables may be accepted or rejected in the sole discretion of the State; and any such alternates or substitutes must be accompanied by Vendor's certification and evidence satisfactory to the State that the function, characteristics, performance and endurance will be equal or superior to the original Deliverables specified.

No response required.

3.1.3 Site and System Preparation

Vendors shall provide the Purchasing State Agency complete site requirement specifications for the Deliverables, if any. These specifications shall ensure that the Deliverables to be installed or implemented shall operate properly and efficiently within the site and system environment. Any alterations or modification in site preparation, which are directly attributable to incomplete or erroneous specifications provided by the Vendor and which would involve additional expenses to the State, shall be made at the expense of the Vendor.

No site or system preparation required.

3.1.4 Equivalent Terms

Whenever a material, article or piece of equipment is identified in the specification(s) by reference to a manufacturers or Vendor's name, trade name, catalog number or similar identifier, it is intended to establish a standard for determining substantial conformity during evaluation, unless otherwise specifically stated as a brand specific requirement (no substitute items will be allowed). Any material, article or piece of equipment of other manufacturers or Vendors shall perform to the standard of the item named. Equivalent offers must be accompanied by sufficient descriptive literature and/or specifications to provide for detailed comparison.

No response required.

3.1.5 Enterprise Licensing

In offering the best value to the State, Vendors are encouraged to leverage the State's existing resources and license agreements, which can be viewed here: <https://it.nc.gov/resources/statewide-it-procurement/statewide-it-contracts>

- a) Identify components or products that are needed for your solution that may not be available with the State's existing license agreement.
 - b) Identify and explain any components that are missing from the State's existing license agreement.
 - c) If the Vendor can provide a more cost-effective licensing agreement, please explain in detail the agreement and how it would benefit the State.
-



3.2 Security Requirements and Specifications

The State is seeking a solution that is either hosted on State Infrastructure or hosted on Vendor provided Infrastructure depending on the solution the Vendor recommends.

3.2.1 Solutions Hosted on State Infrastructure

In line with our recommendations, our solutions are exclusively hosted on Vendor-provided Infrastructure. Therefore, this section pertaining to solutions hosted on State Infrastructure is not applicable to our proposal.

3.2.2 Solutions Not Hosted on State Infrastructure



3.3 Enterprise Specifications

3.3.1 Enterprise Strategies, Services, and Standards

Agencies and vendors should refer to the Vendor Resources Page for information on North Carolina Information Technology enterprise services, security policies and practices, architectural requirements, and enterprise contracts. The Vendor Resources Page can be found at the following link: <https://it.nc.gov/vendor-engagement-resources>. This site provides vendors with statewide information and links referenced throughout the RFP document. Agencies may request additional information.

No response required.

3.3.2 Architecture Diagrams Defined

The State utilizes architectural diagrams to better understand the design and technologies of a proposed solution. These diagrams (i.e., Network Diagram and Technology Stack Diagram), required at offer submission, can be found at the following link: <https://it.nc.gov/architectural-artifacts>. There may be additional architectural diagrams requested of the vendor after contract award. This will be communicated to the vendor by the agency as needed during the project.

Please refer to **Section F - Architecture Diagrams**.

3.3.3 Virtualization

The State desires the flexibility to host Vendor's proposed solution in a virtualized environment, should it determine in the future that virtualized hosting for such solution would be more economical or efficient. The State currently utilizes server virtualization technologies including VMware, Solaris and Linux. The Vendor should state whether its solution operates in a virtualized environment. Vendor also should identify and describe all differences, restrictions or limitations of its proposed solution with respect to operation, licensing, support, certification, warranties, and any other details that may impact its proposed solution when hosted in a virtualized environment.

No response required.

3.3.4 Identity and Access Management (IAM)

The proposed solution must externalize identity and access management. The protocols describing the State's Identity and Access Management can be found at the following link: <https://it.nc.gov/services/vendor-engagement-resources#identity-access-management>

Describe how your solution supports the above protocols as well as making them available for application integration/consumption.

NC-PROCEED will integrate with external IAM systems for user authentication and coarse grain authorization.

The solution can integrate with the NCID system, or with the Enterprise Active Directory Services, and can leverage multifactor authentication from the Enterprise Active Directory service.

Salesforce is fully SAML2 compliant and can be configured as a service provider using SAML single sign-on (SSO). NC-PROCEED will be able to externalize IAM by integrating with any SAML2-based identity provider including the State's IAM solution (NCID). This SSO configuration will authenticate users of the licensure system and control access based on the available information provided by the identity management system during the SSO handshake.

Salesforce can also be customized internally using just-in-time (JIT) logic to perform user related logic after a successful SSO login. For example, this feature can be used to synchronize user profile properties between Salesforce and the identity system as well as update Salesforce access controls.

3.4 Business and Technical Specifications

Refer to the following attachments:

ATTACHMENT K, REGULATORY MODERNIZATION BUSINESS SPECIFICATIONS

ATTACHMENT L, WORKFORCE REGISTRY BUSINESS SPECIFICATIONS

ATTACHMENT M, NC PRE-K SPECIFICATIONS

ATTACHMENT N, SUBSIDY PROVIDER COMPLIANCE BUSINESS SPECIFICATIONS

SEE ATTACHMENT O. BUSINESS AND TECHNICAL SPECIFICATIONS

3.4.1 Attachment K, Regulatory Modernization Business Specifications

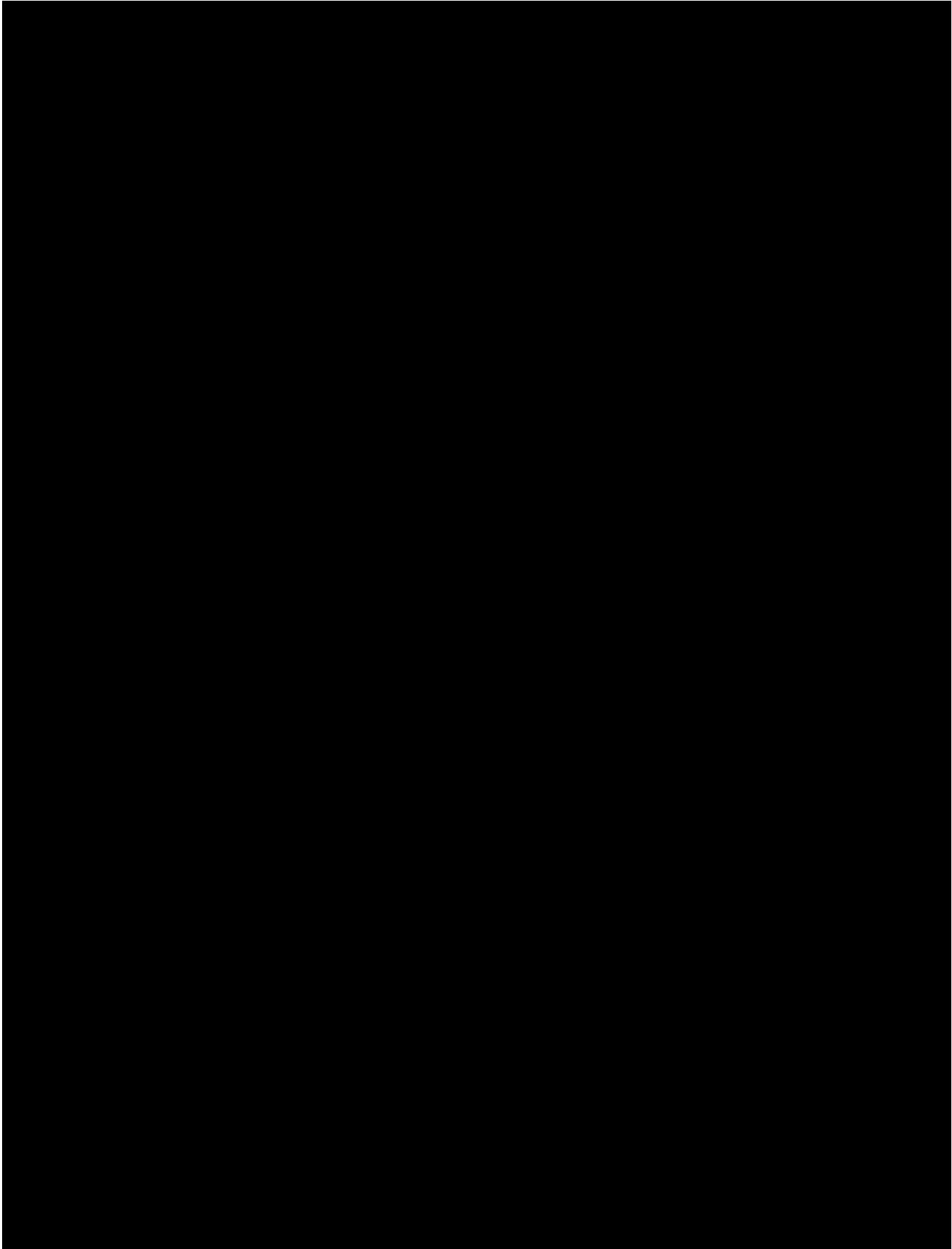
Having collaborated with DCDEE on two prior system deployments, Accenture has a deep understanding of its regulatory framework. This positions us ideally to assist the Division in updating its regulatory system and enhancing its integrations.

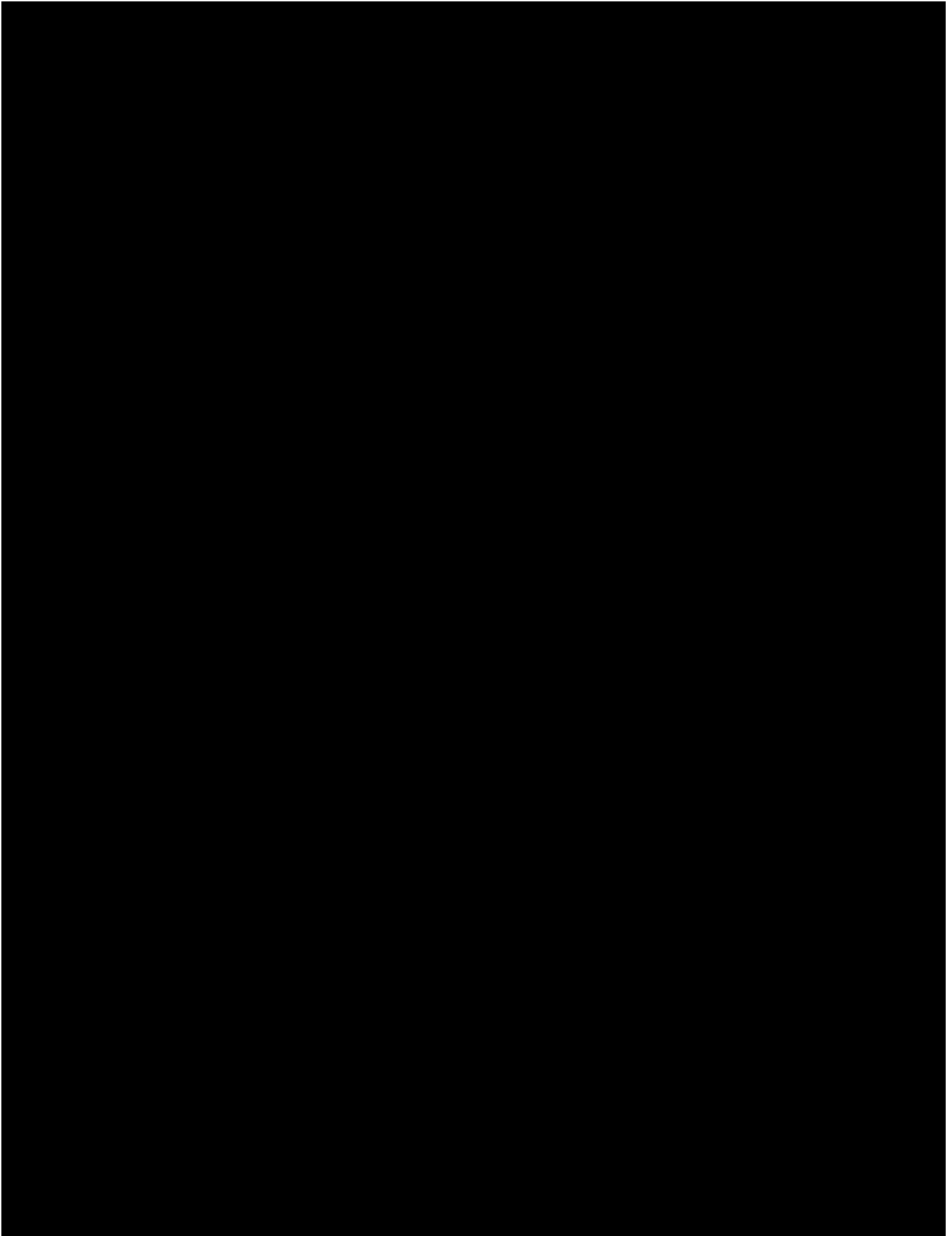
During the implementation of the Subsidized Child Care Assistance program into NC FAST, Accenture developed a seamless integration between the Regulatory system and NC FAST. In the process, we gained a deep understanding of the Regulatory provider data, facilitating a daily data transfer between the systems. This ensured that NC FAST consistently had accurate licensure data to support the SCCA program effectively. Collaborating with DCDEE allowed Accenture to become proficient in distinguishing between centers and family childcare homes, understanding the star rating procedures and regulations, and recognizing the importance of administrative actions.

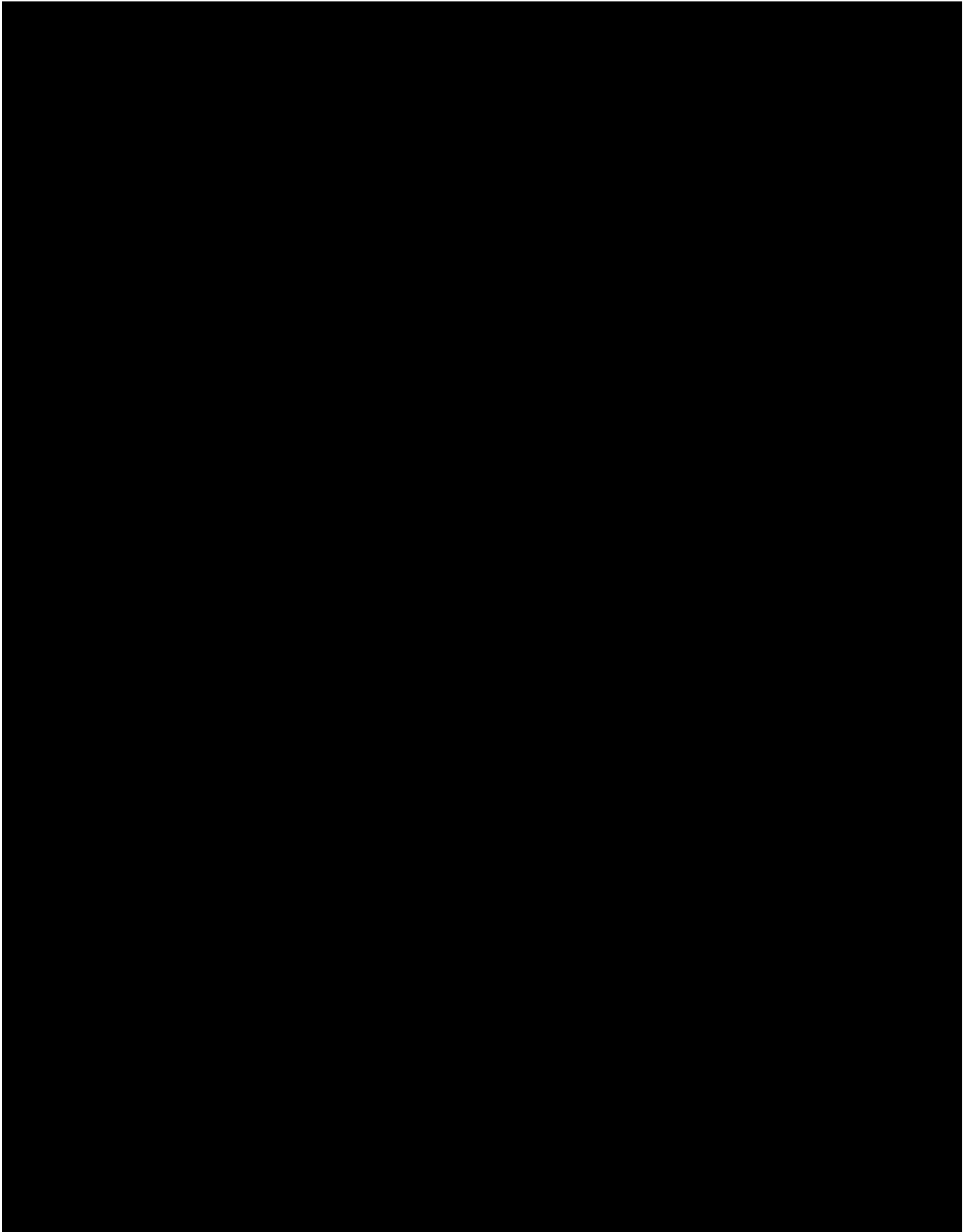
During the creation of the COVID-19 Emergency Child Care Subsidy Provider Portal, Accenture utilized its deep understanding and extensive Salesforce proficiency to assist DCDEE in developing an efficient, user-centric portal within three weeks, promptly addressing the challenges presented by the pandemic.

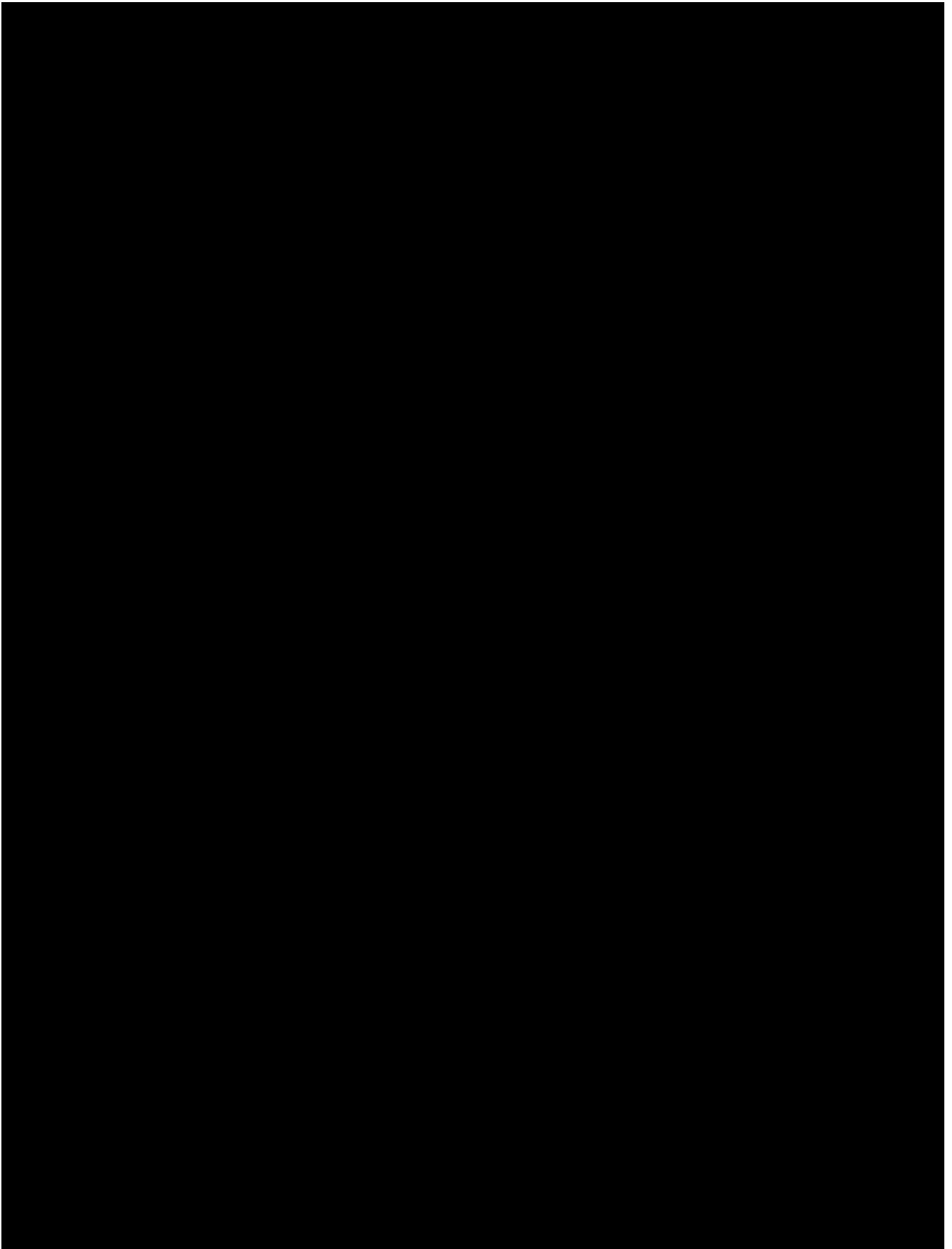
By collaborating with Accenture, DCDEE can anticipate this caliber of expertise to be consistently leveraged, ensuring the Division rolls out a quality product for business modernization and offers an impeccable user experience for the providers it serves.

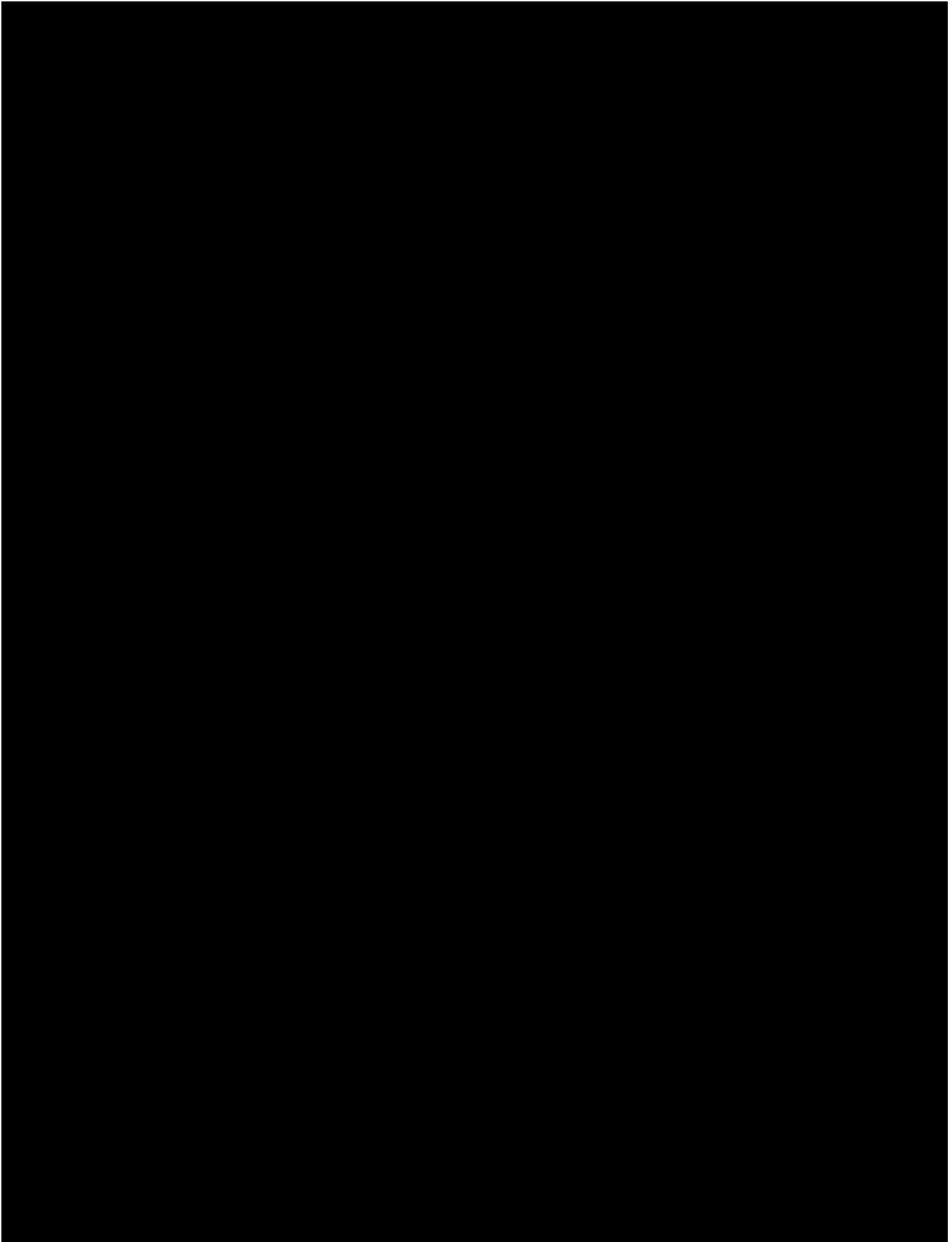
ID	Specification
Authentication	
Auth_1	Describe how the proposed solution will externalize identity management, utilize the North Carolina Identity Service (NCID) for the identity management and authentication related functions. NCID is the State's enterprise identity management (IDM) service. It is operated by the North Carolina Department of Information Technology.
	[REDACTED]
	[REDACTED]
	[REDACTED]

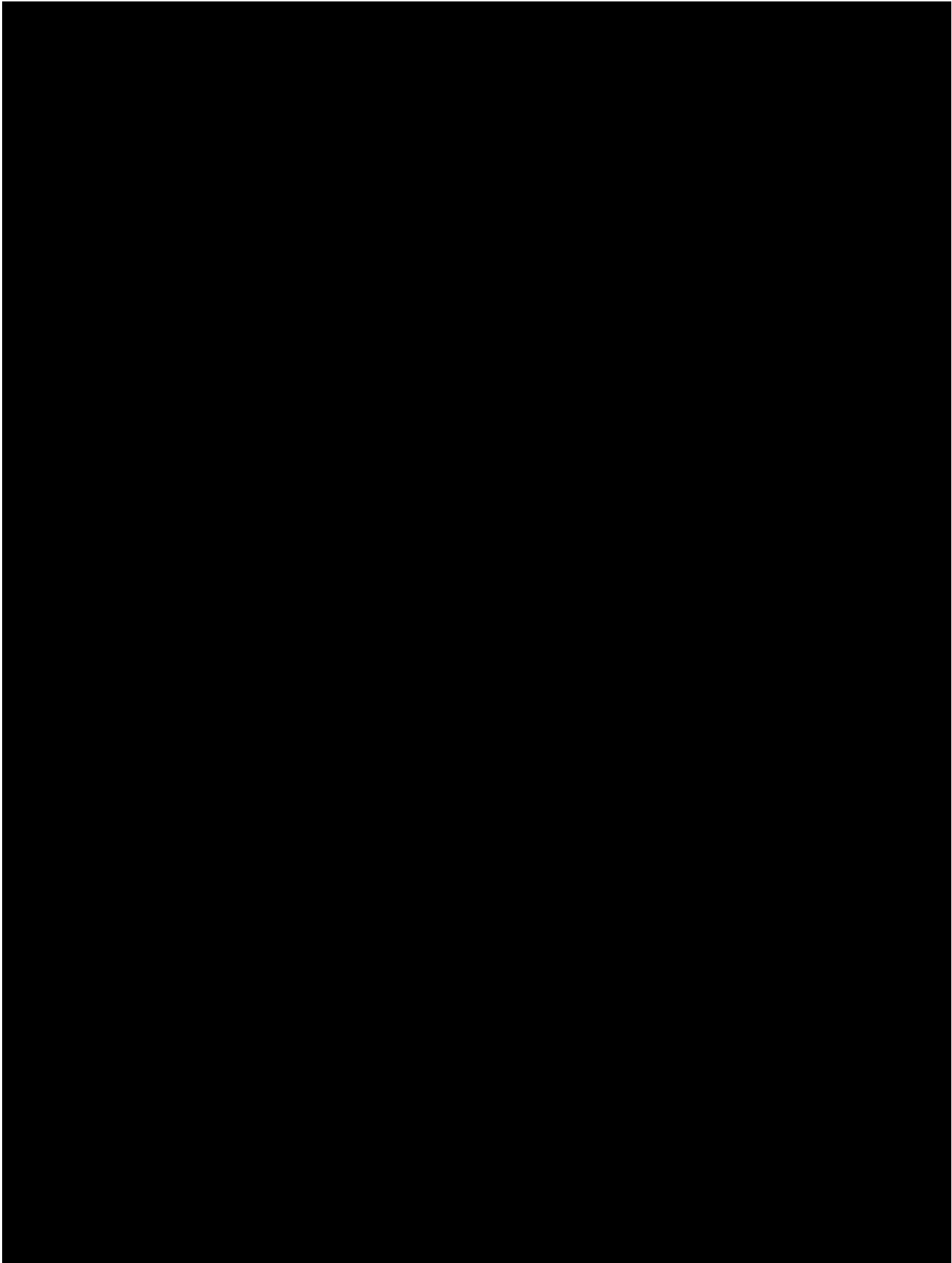


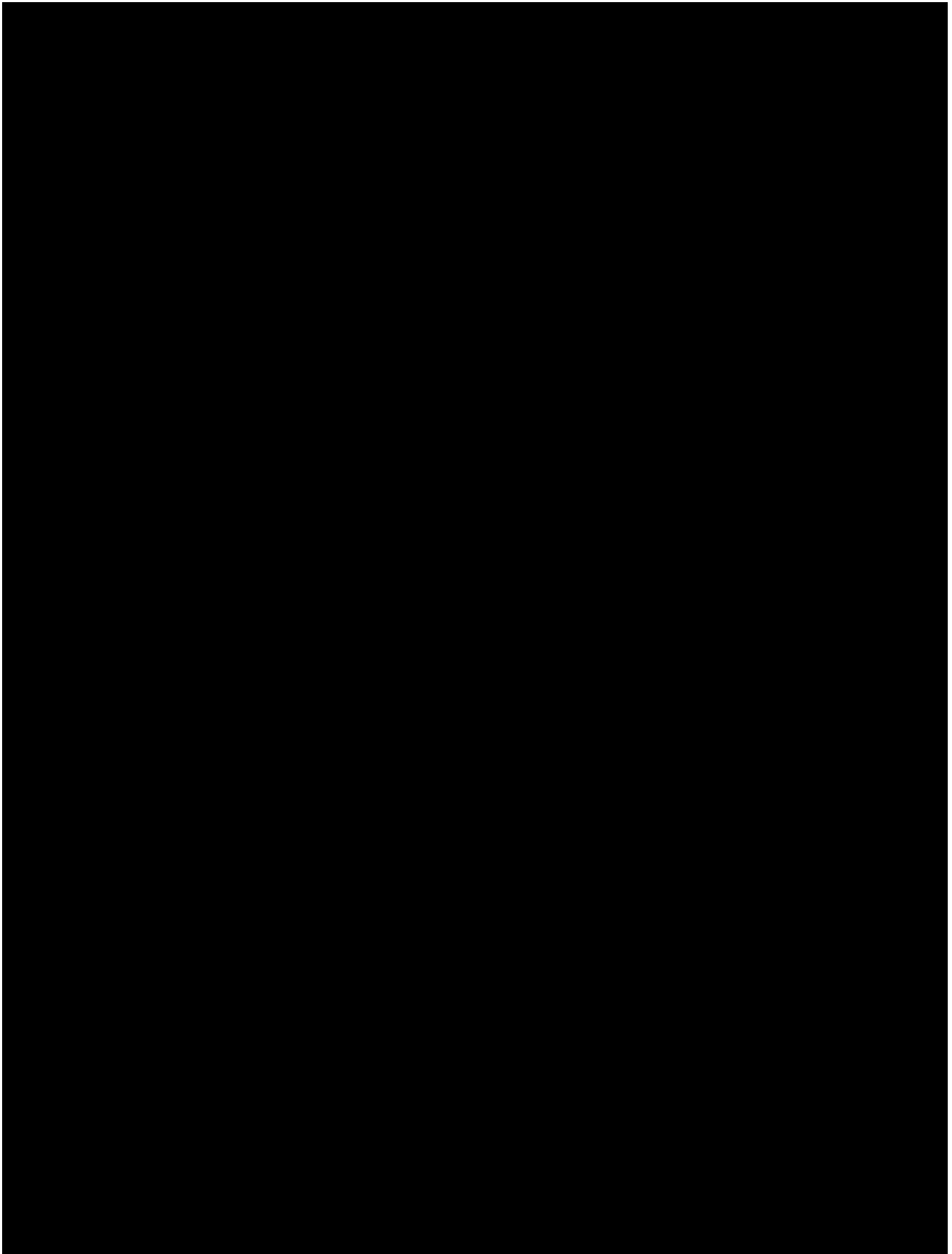


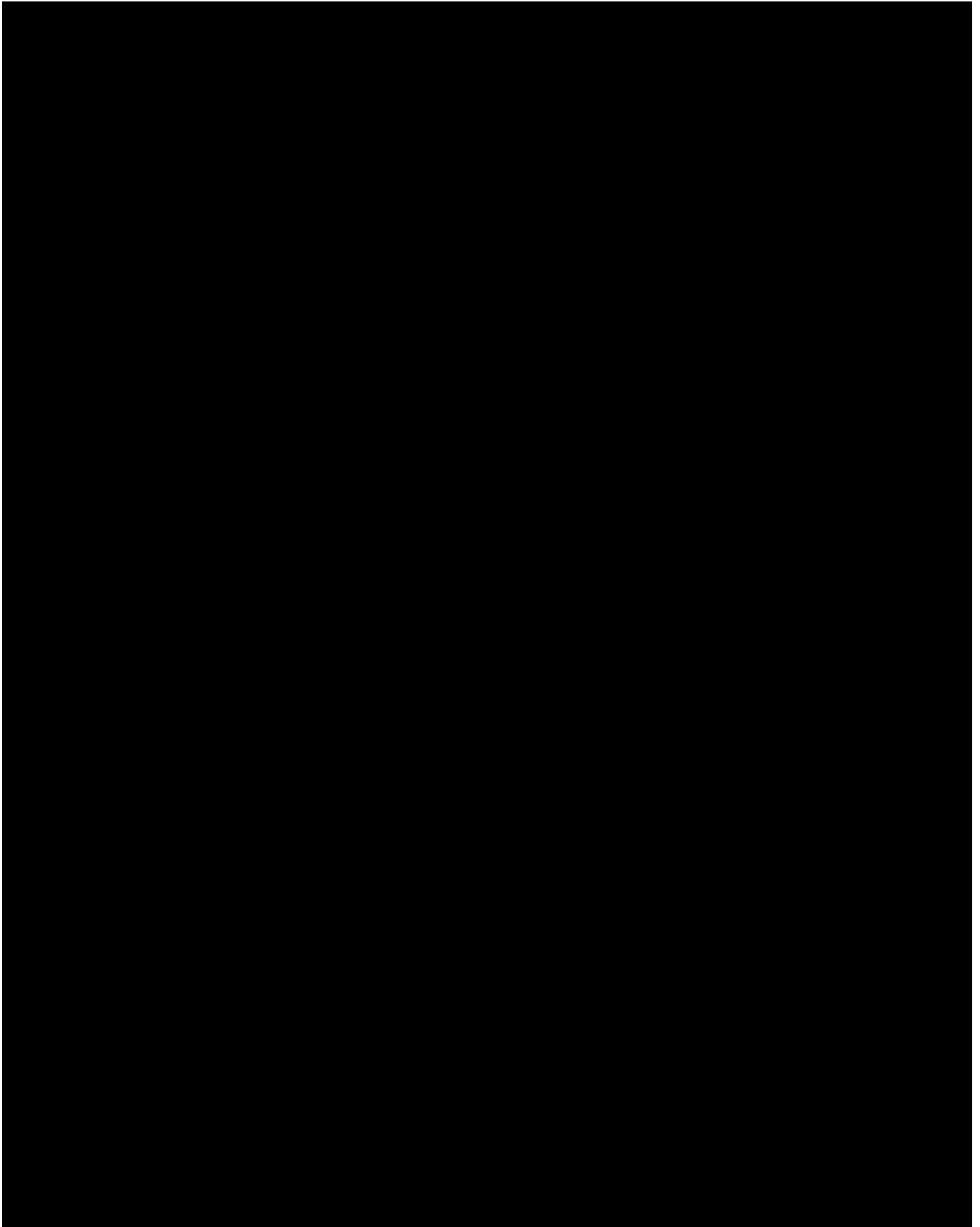


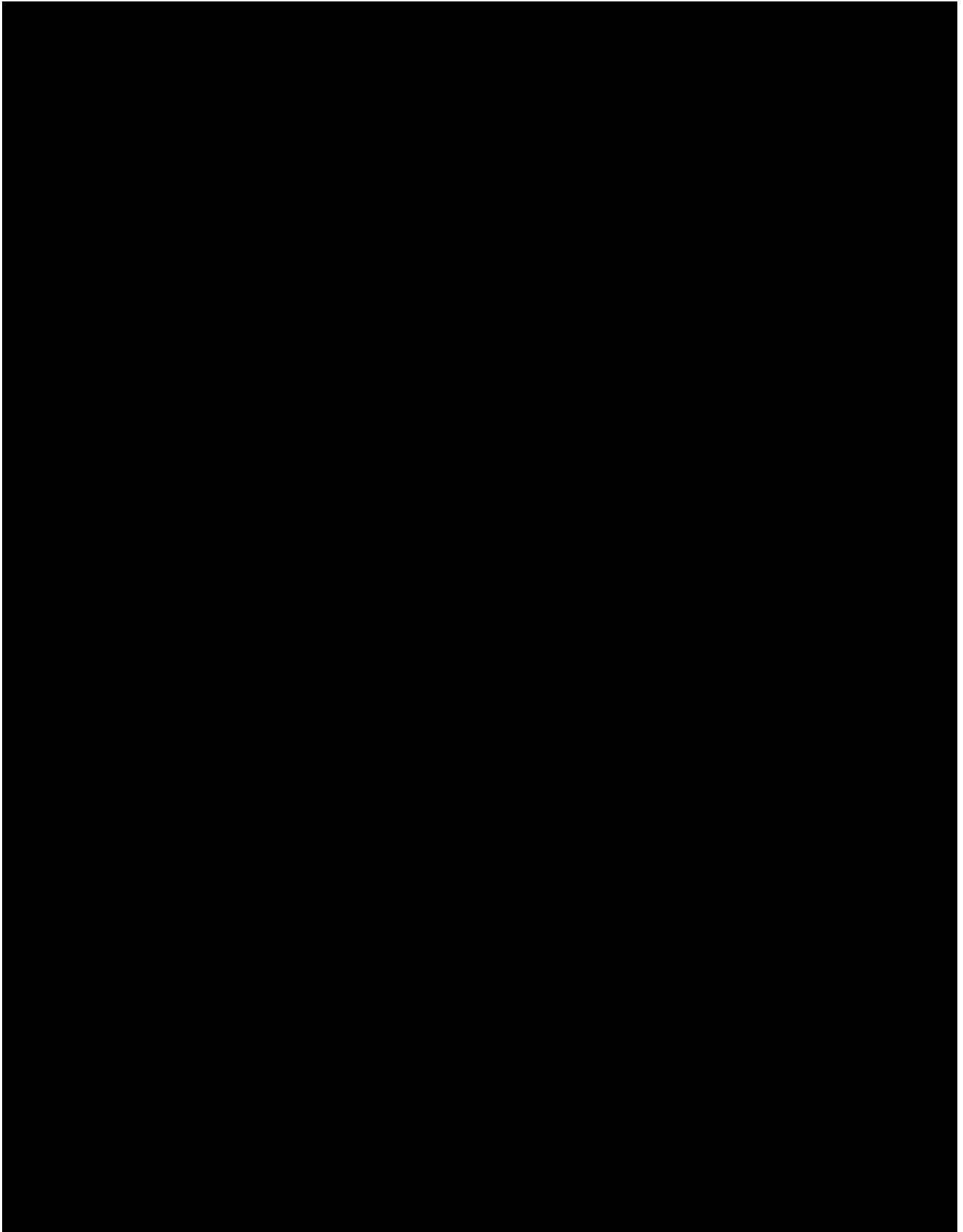


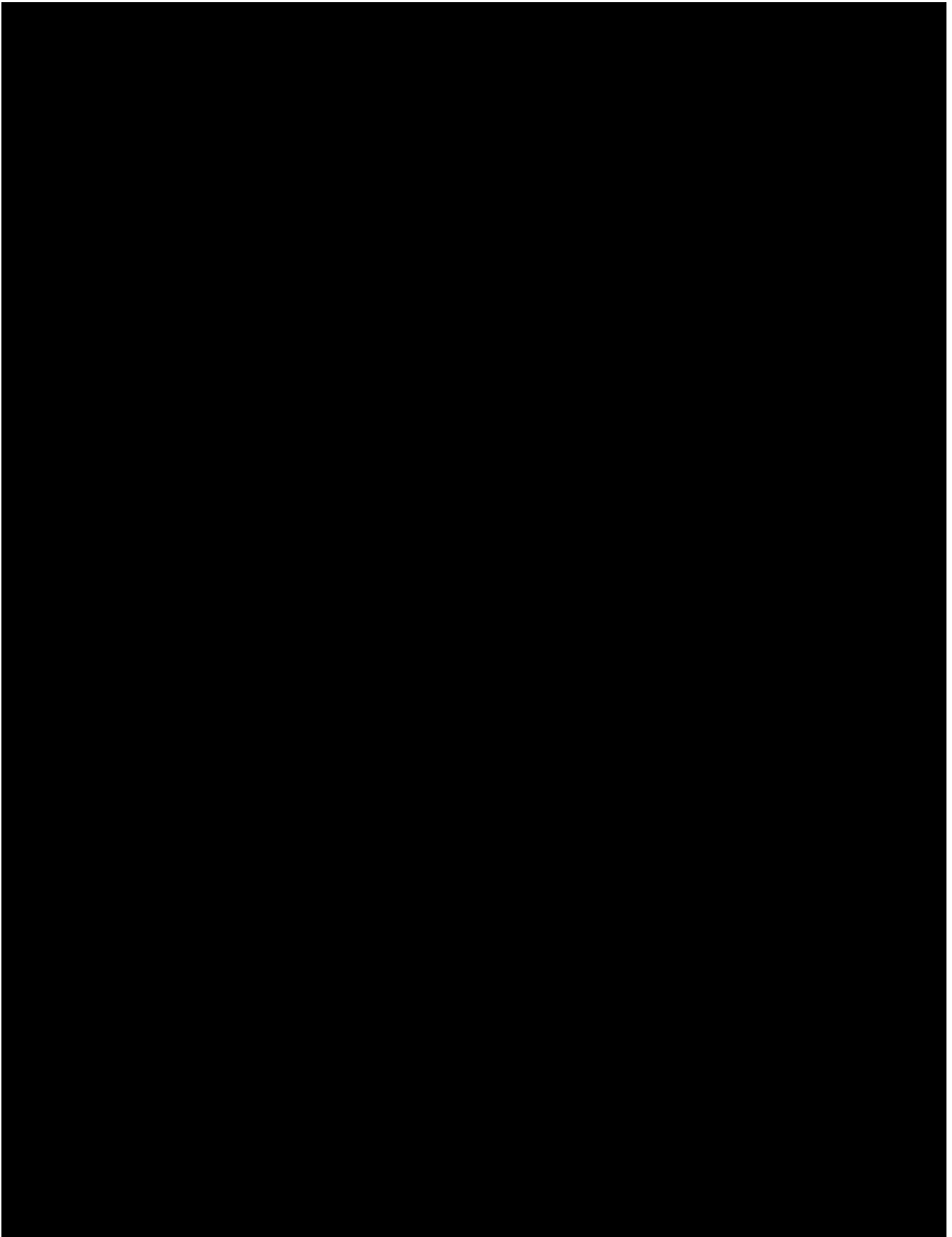


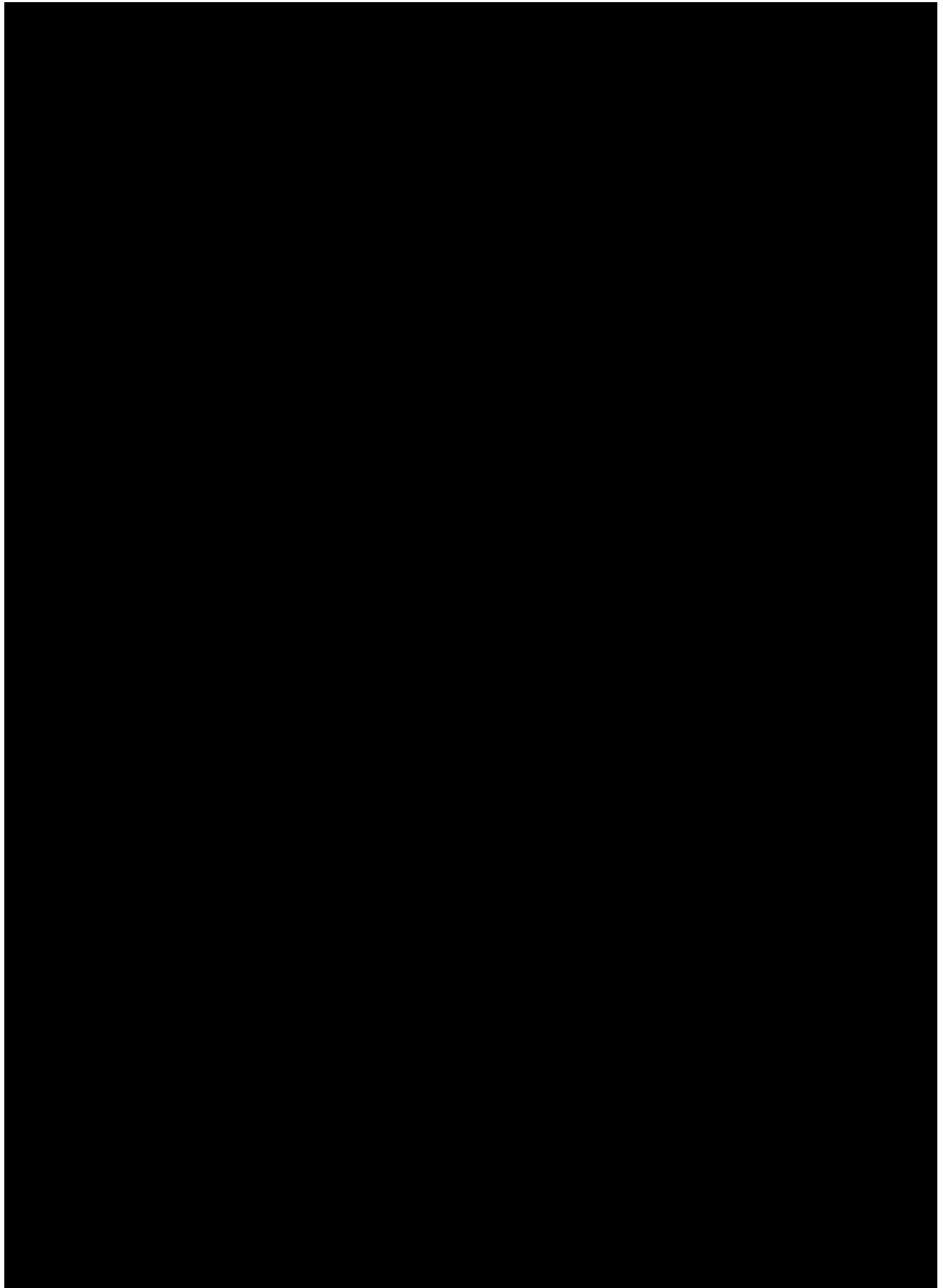


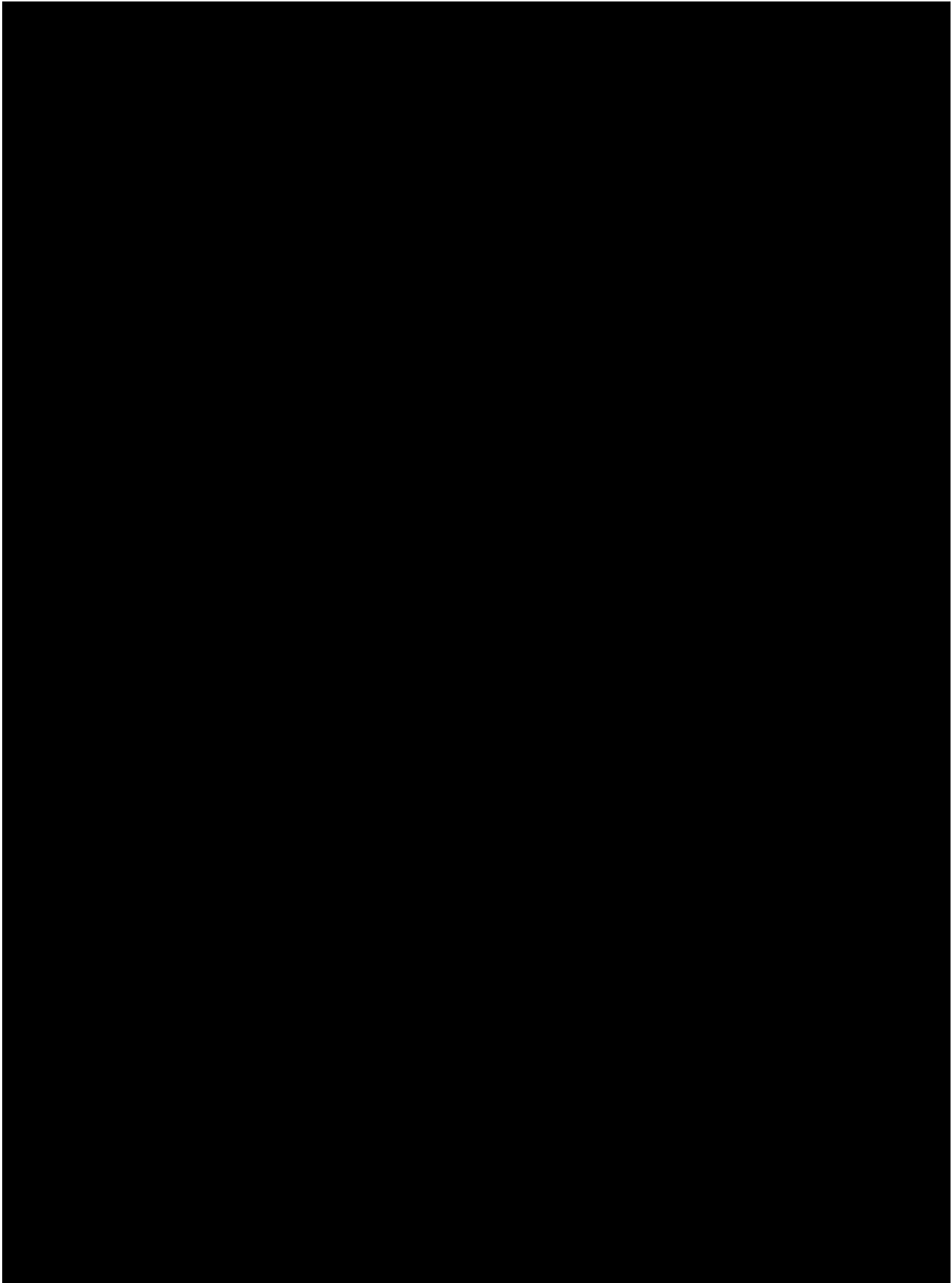


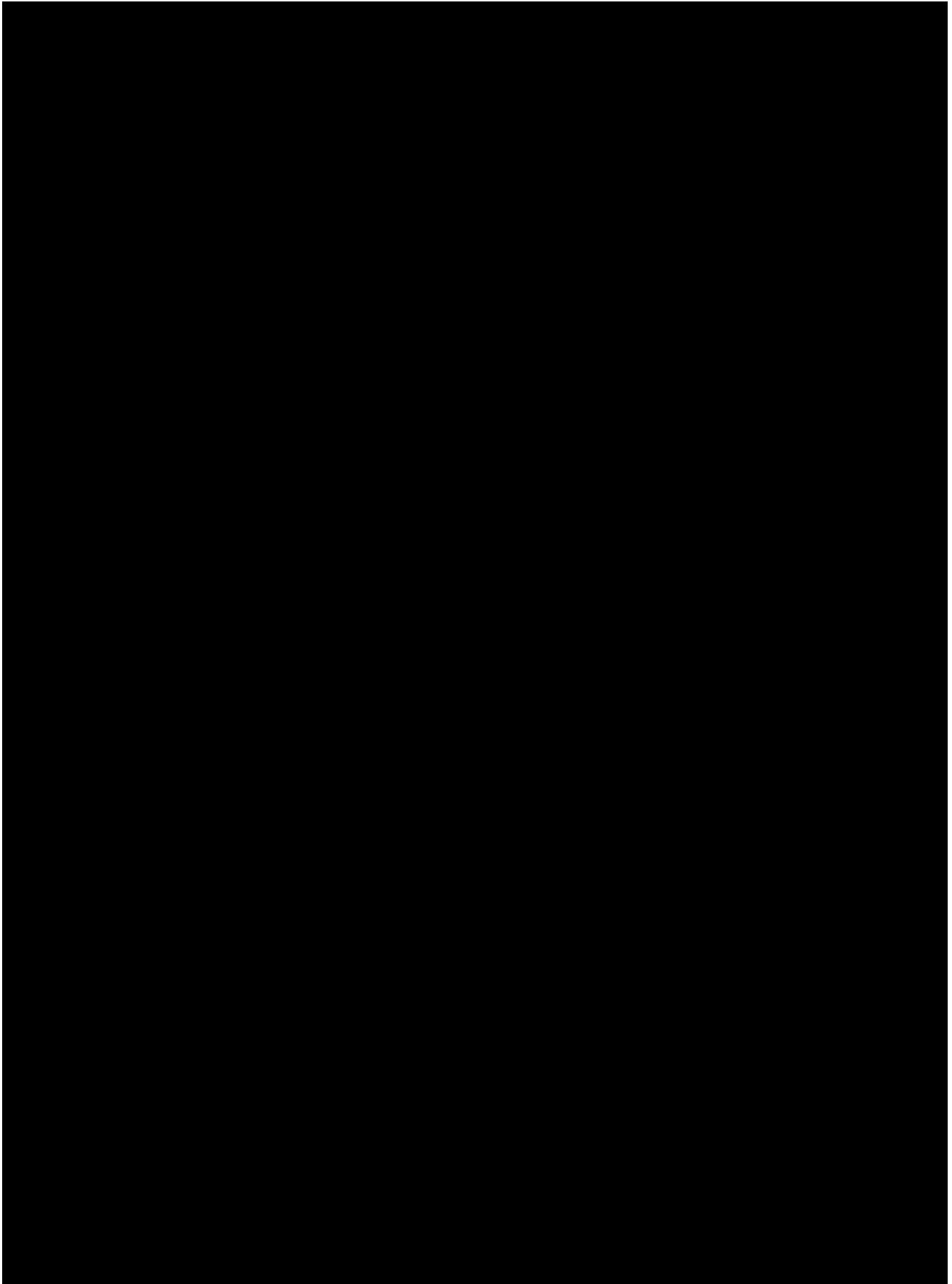


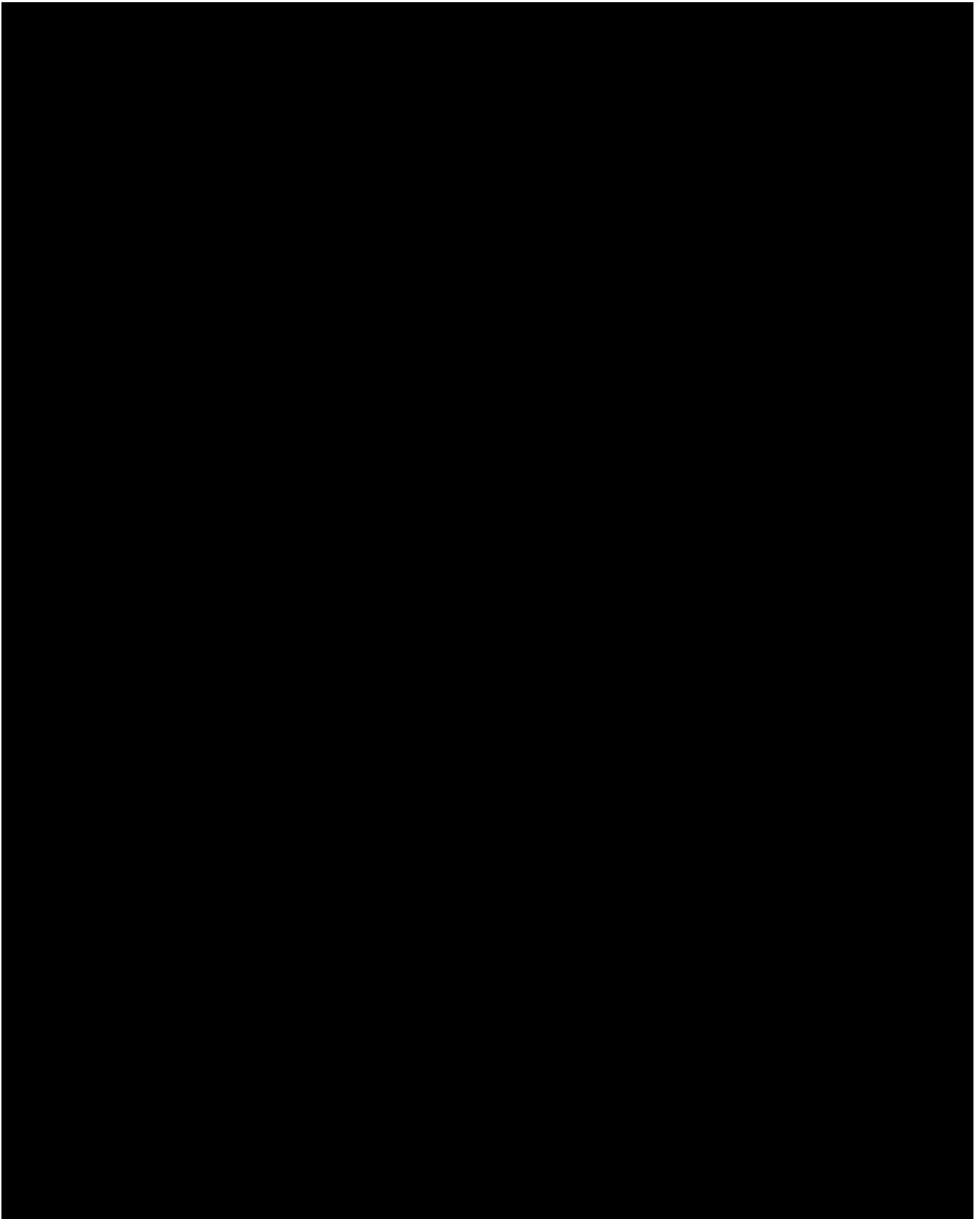


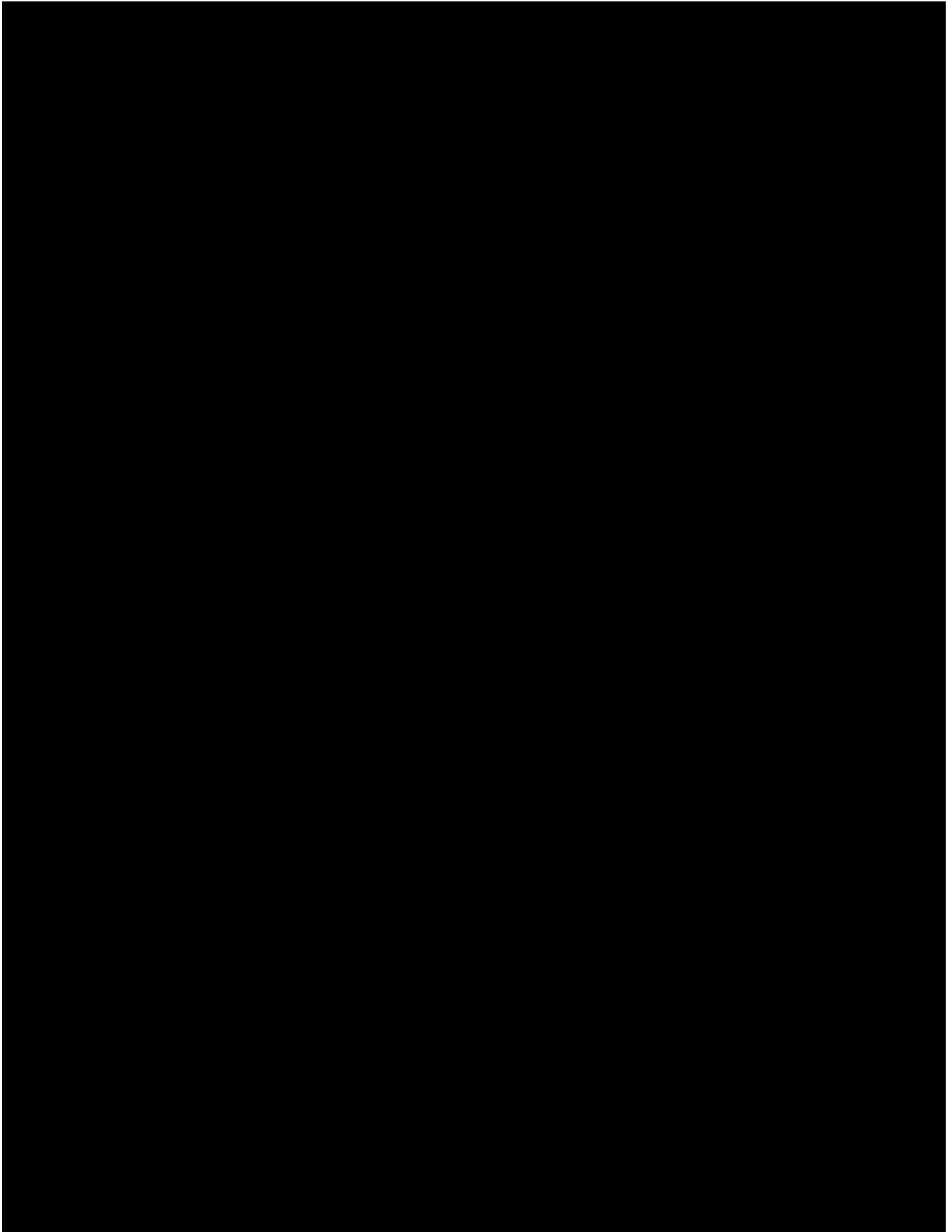


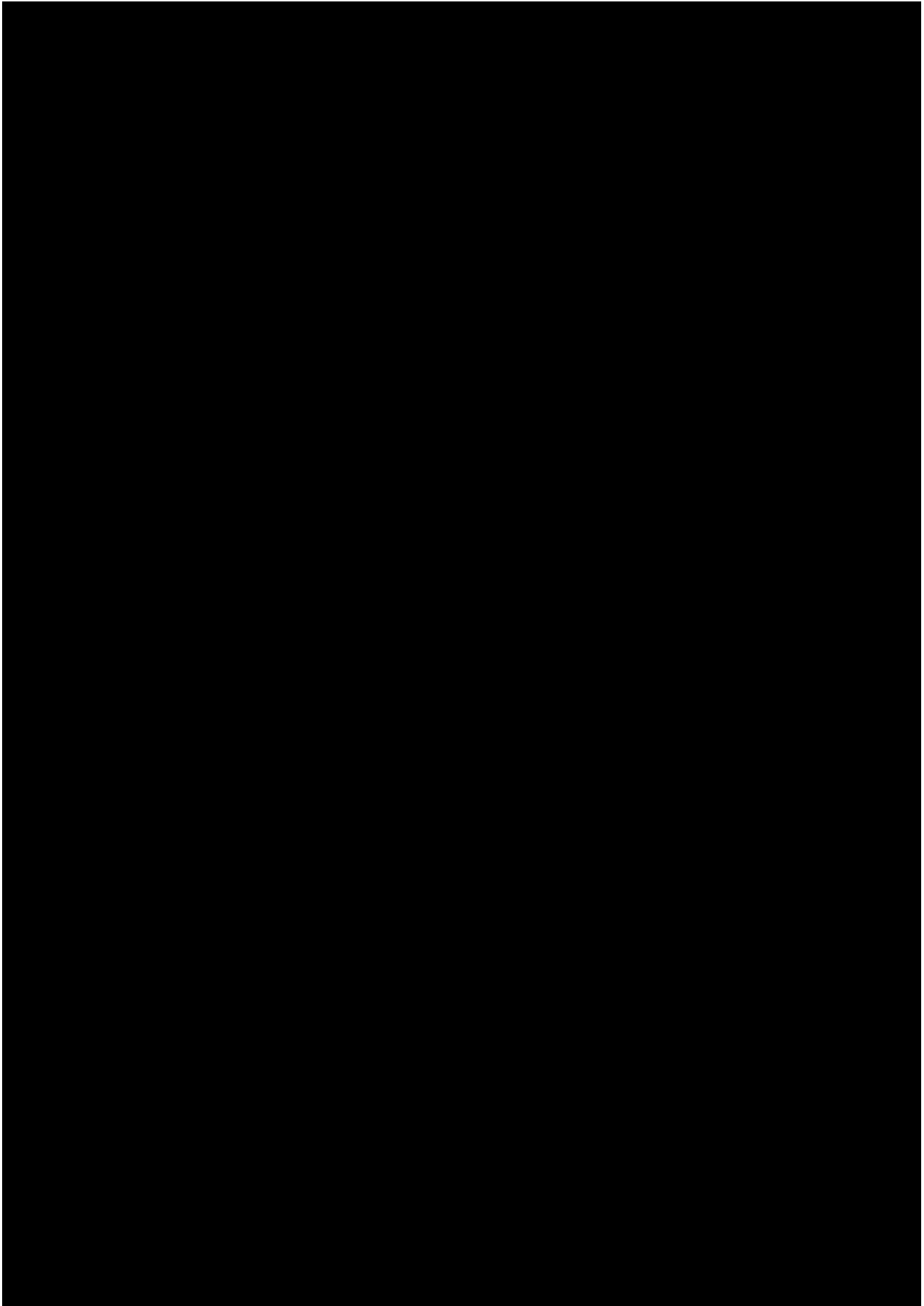


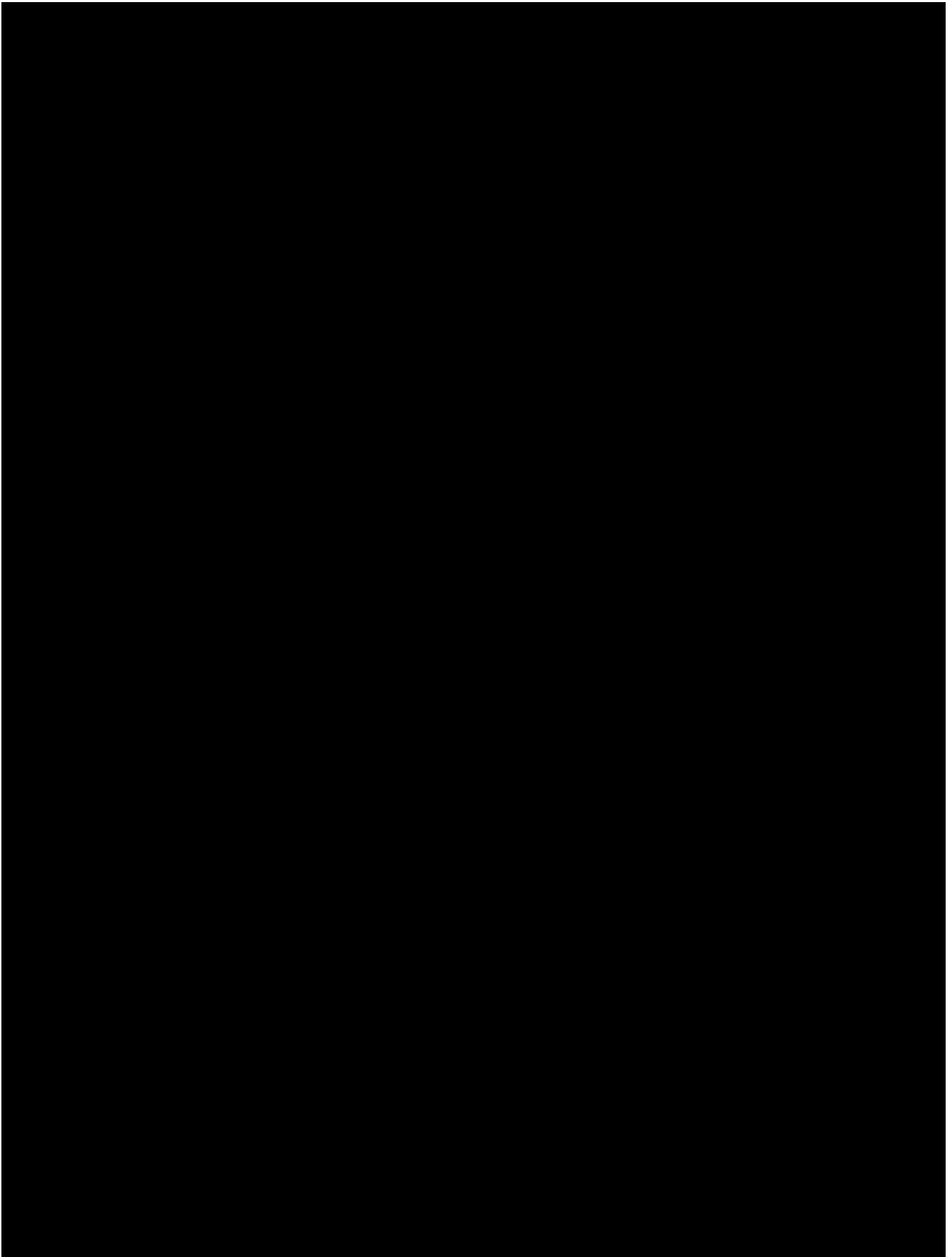


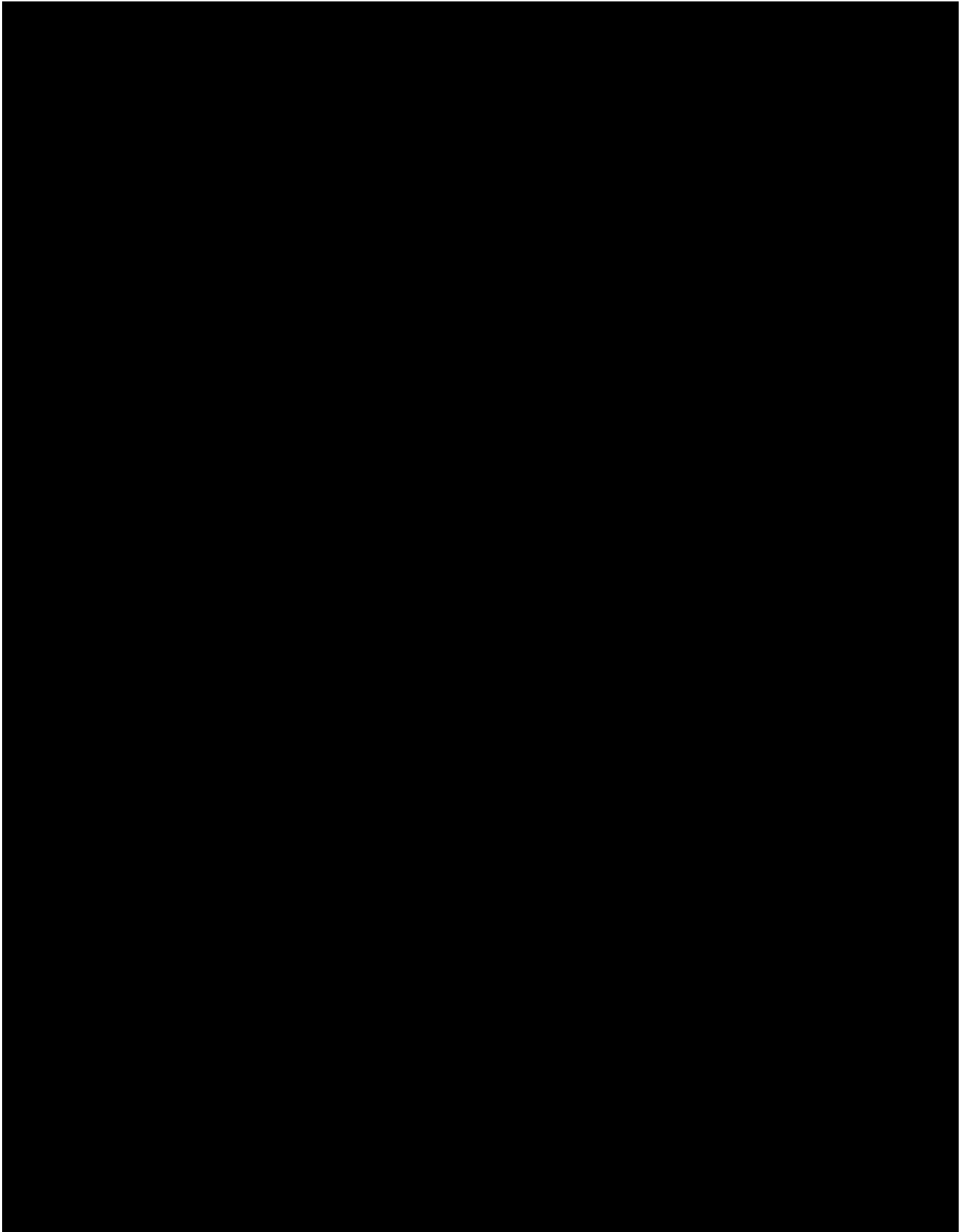


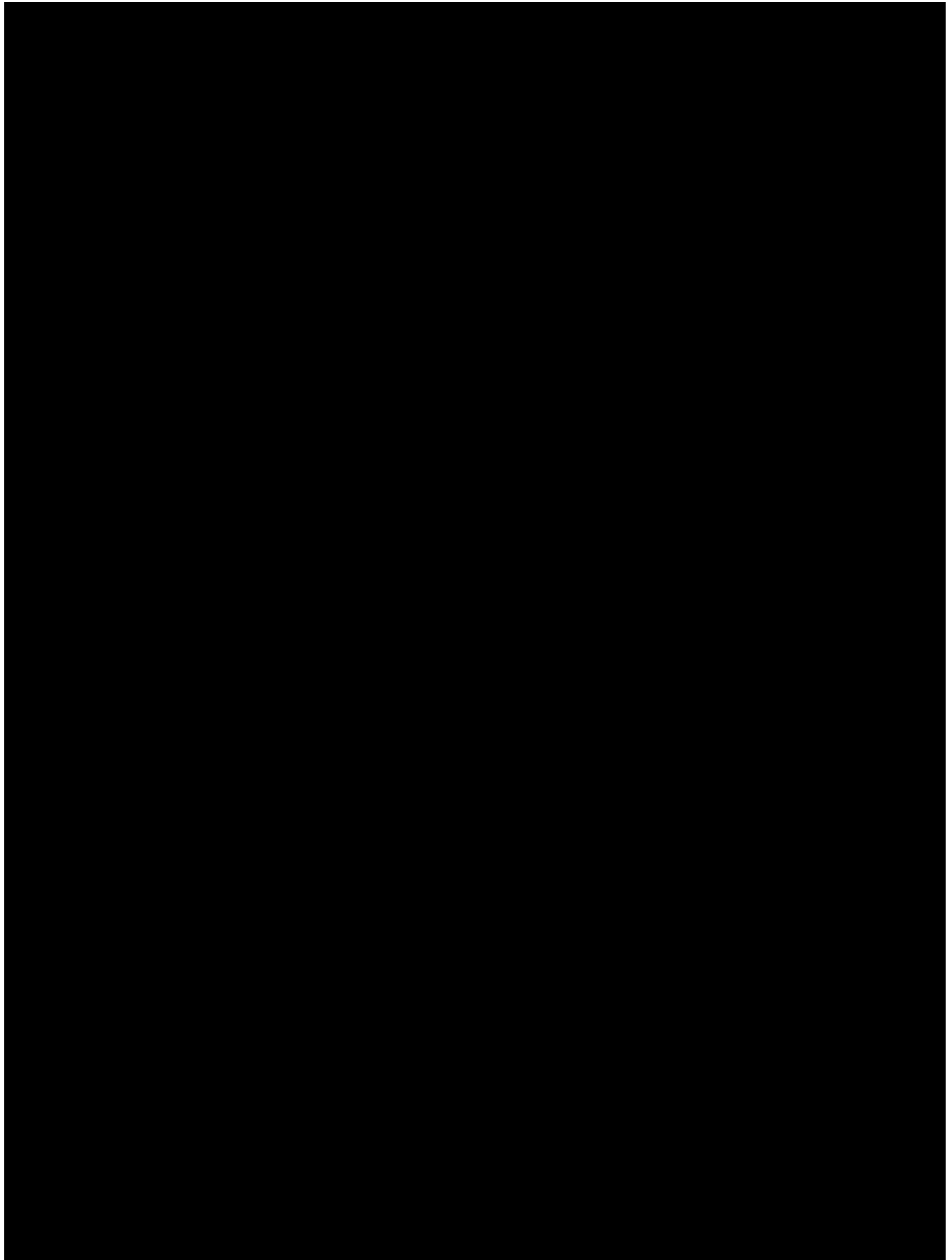


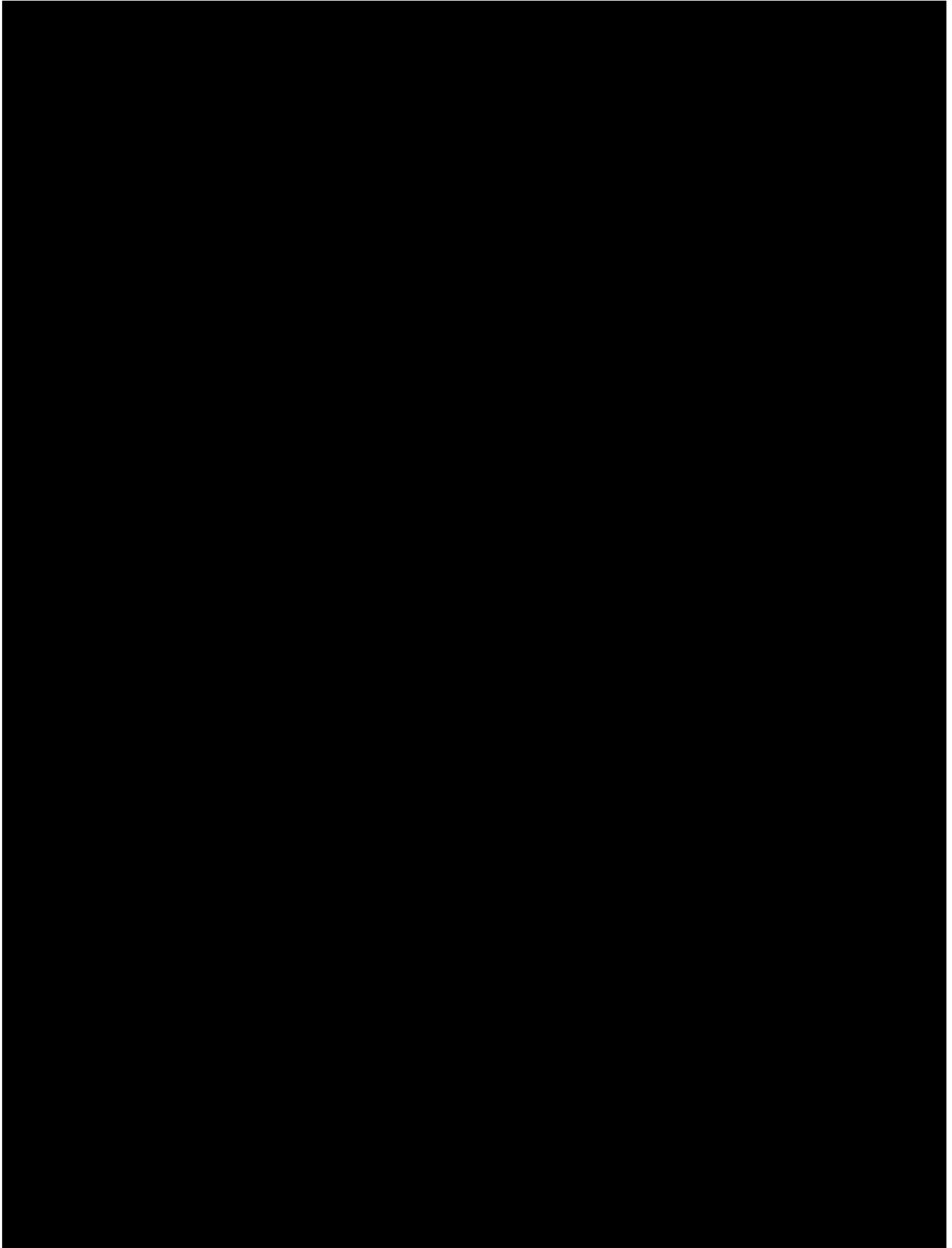


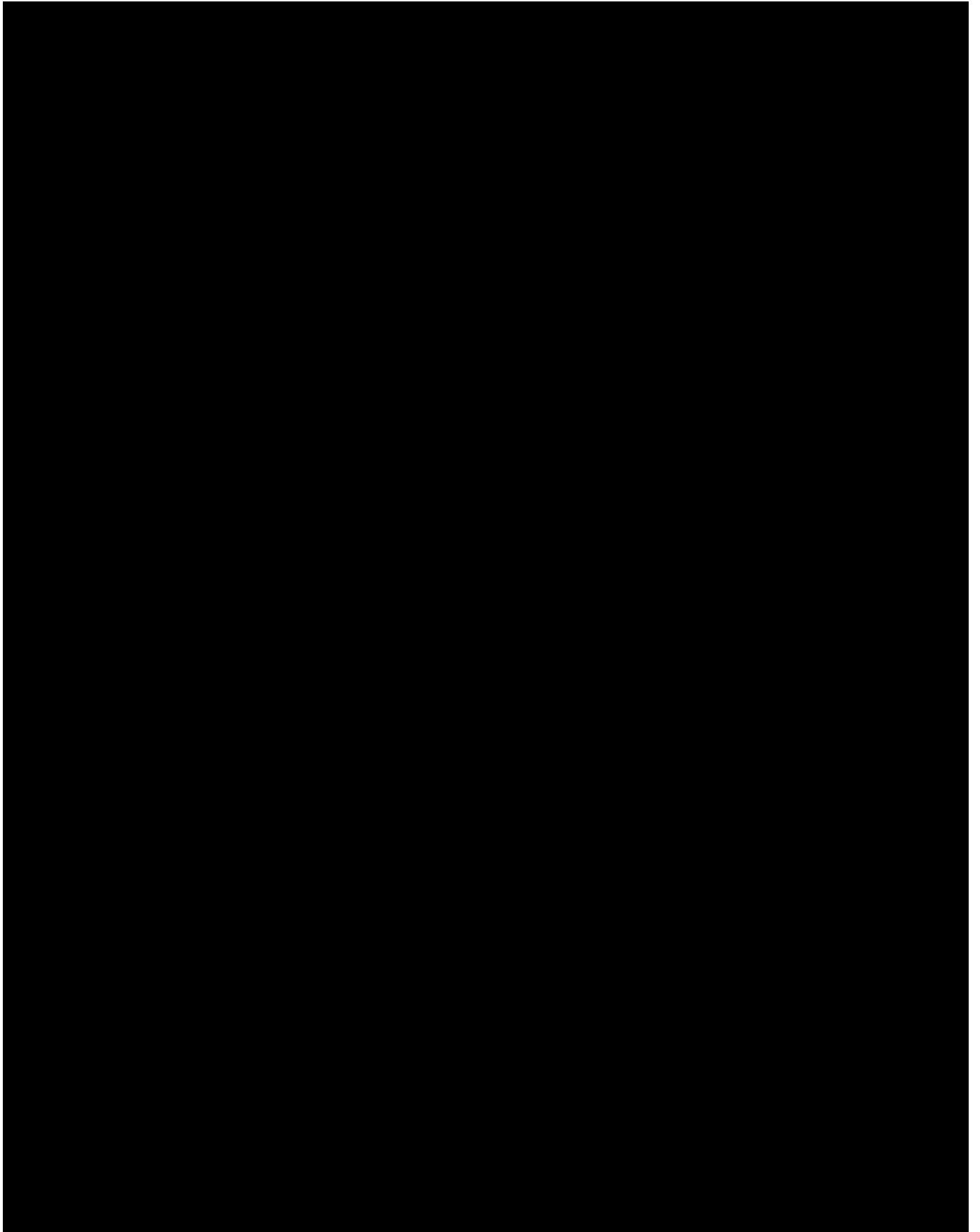


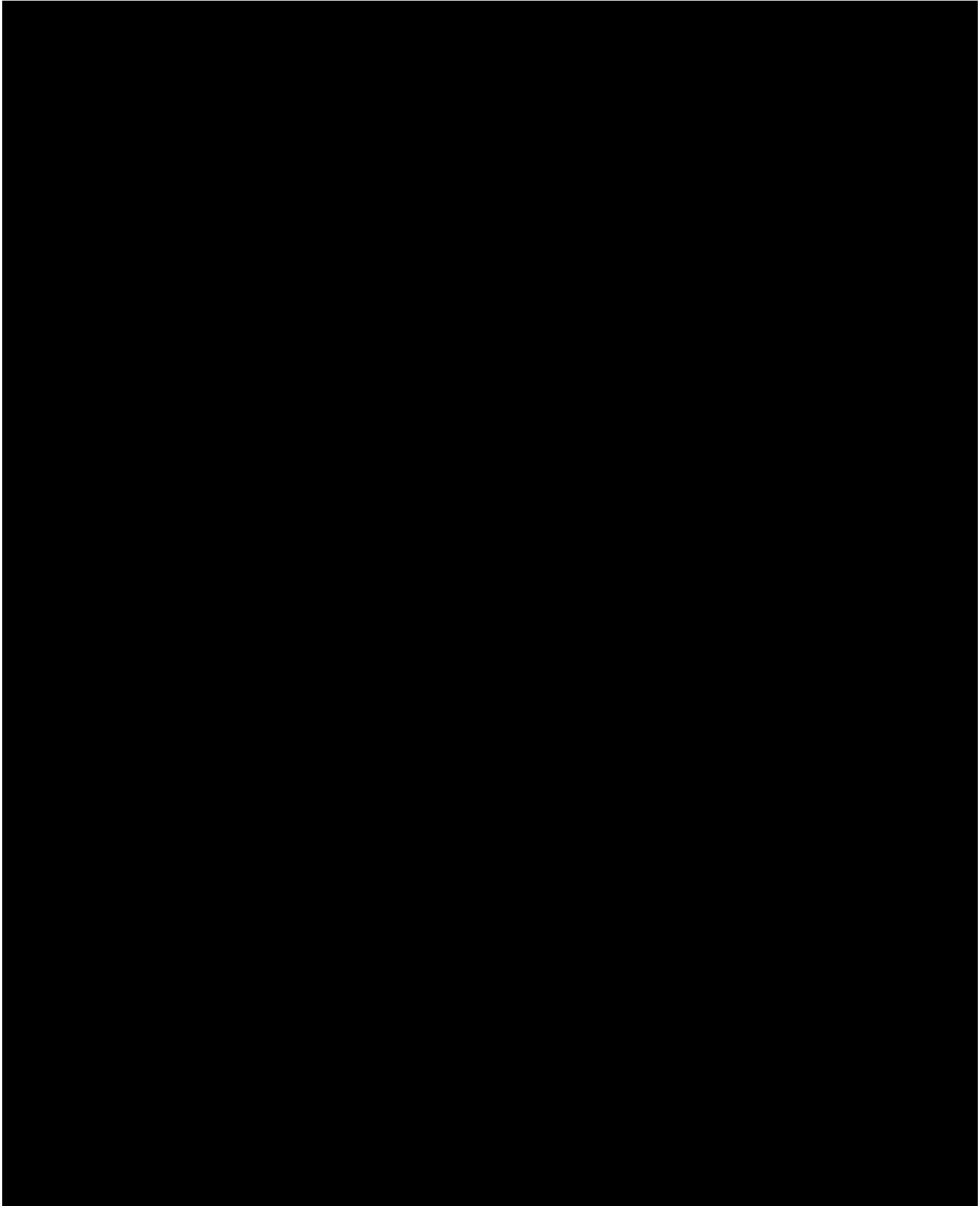


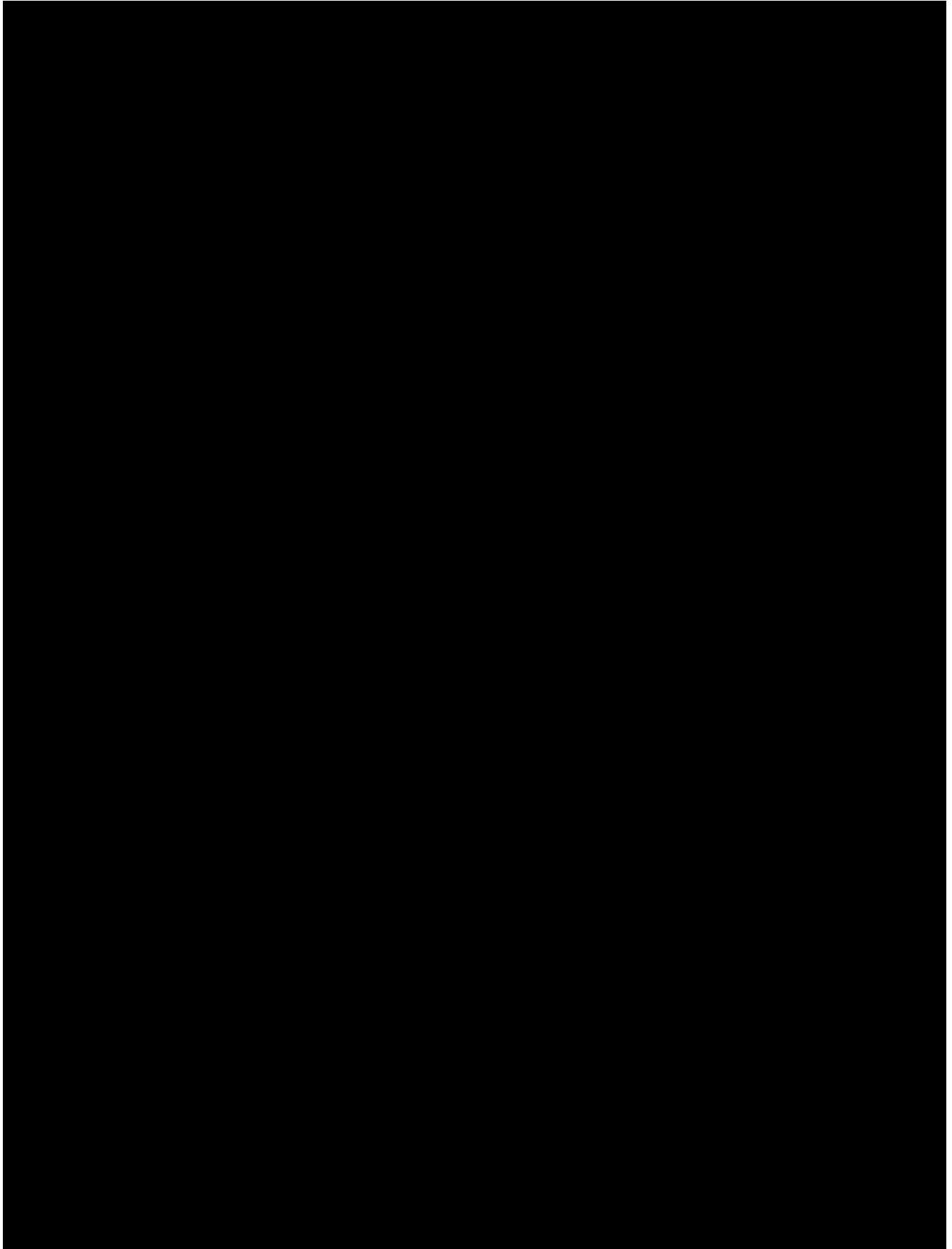


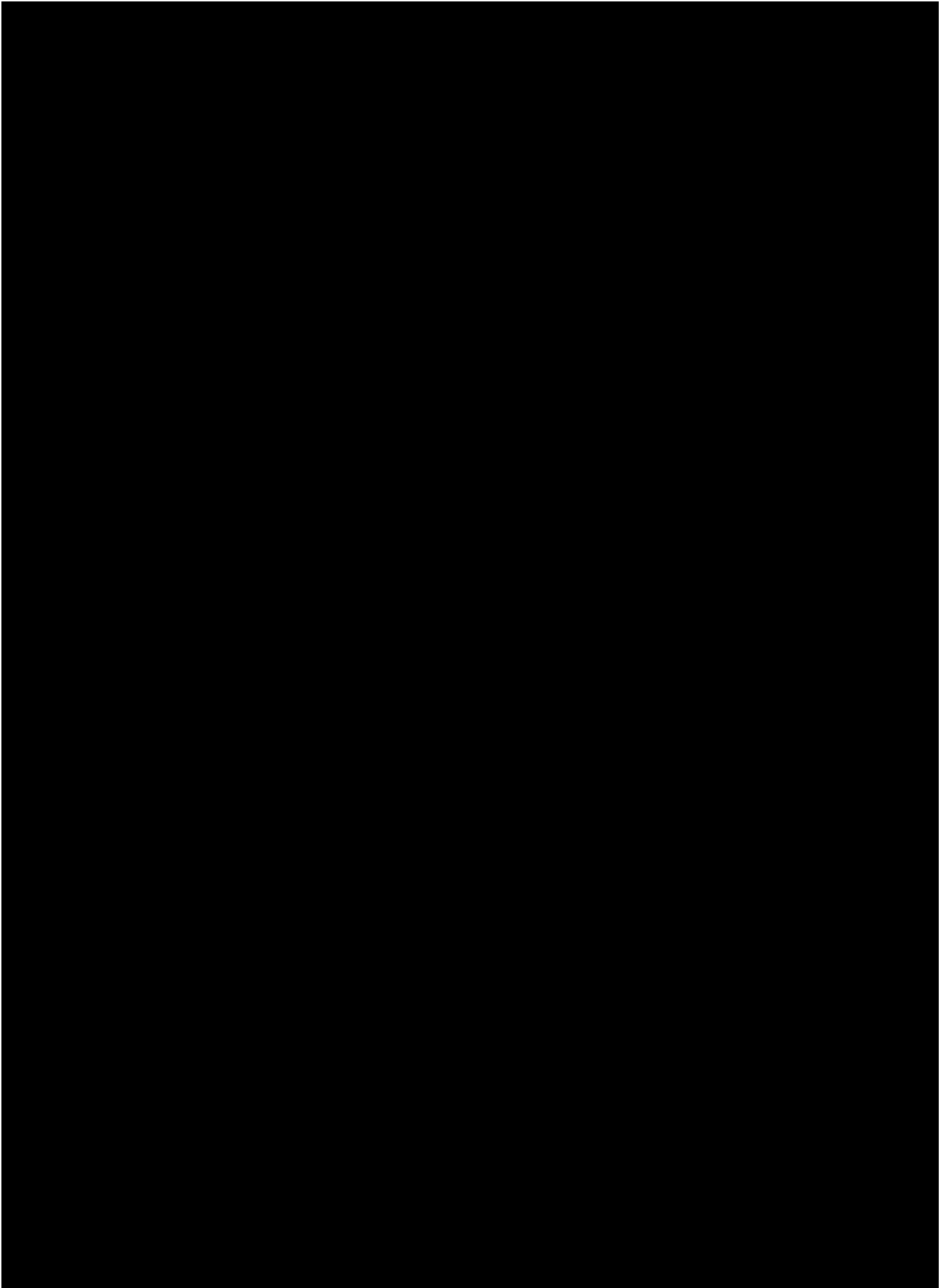


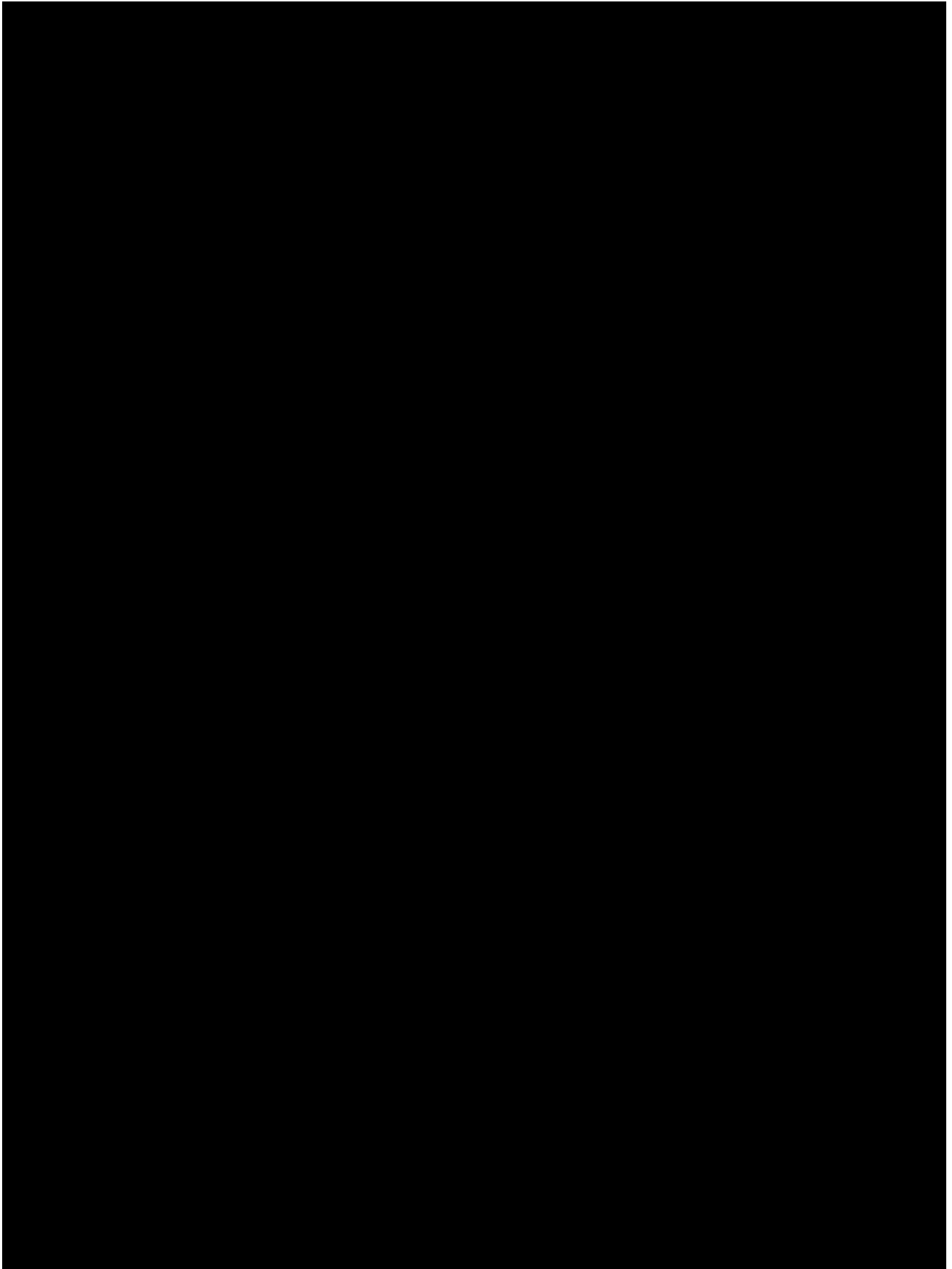


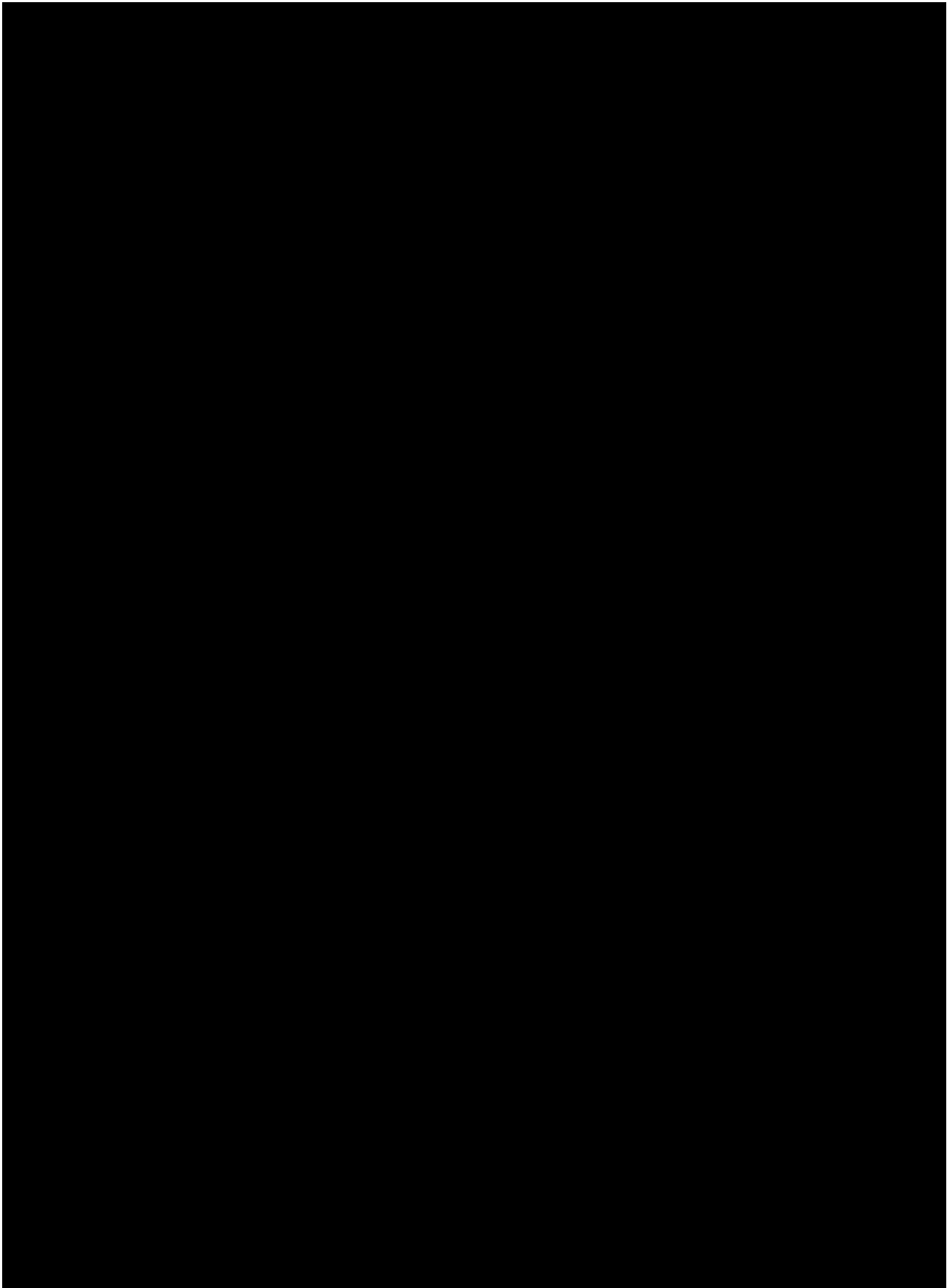


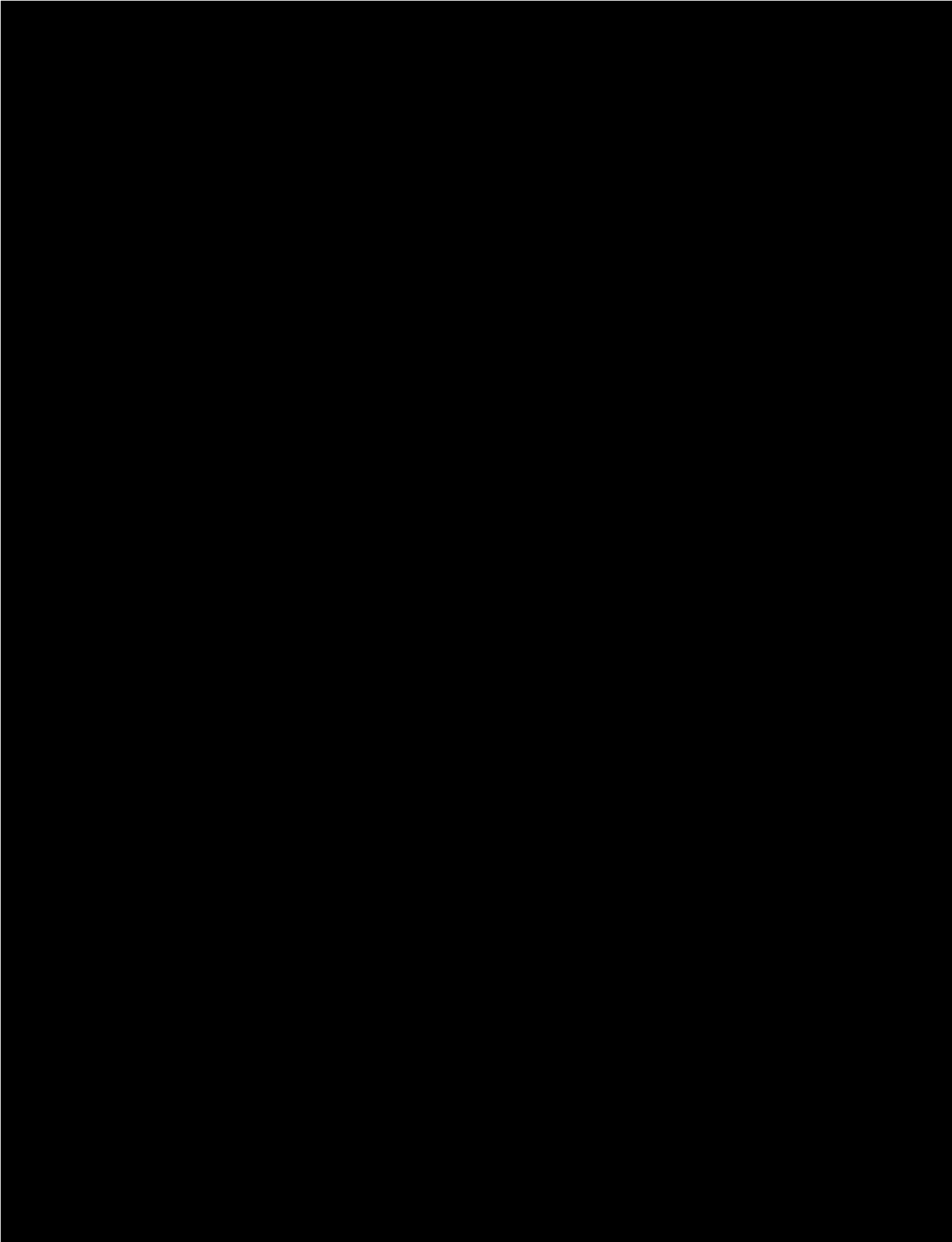


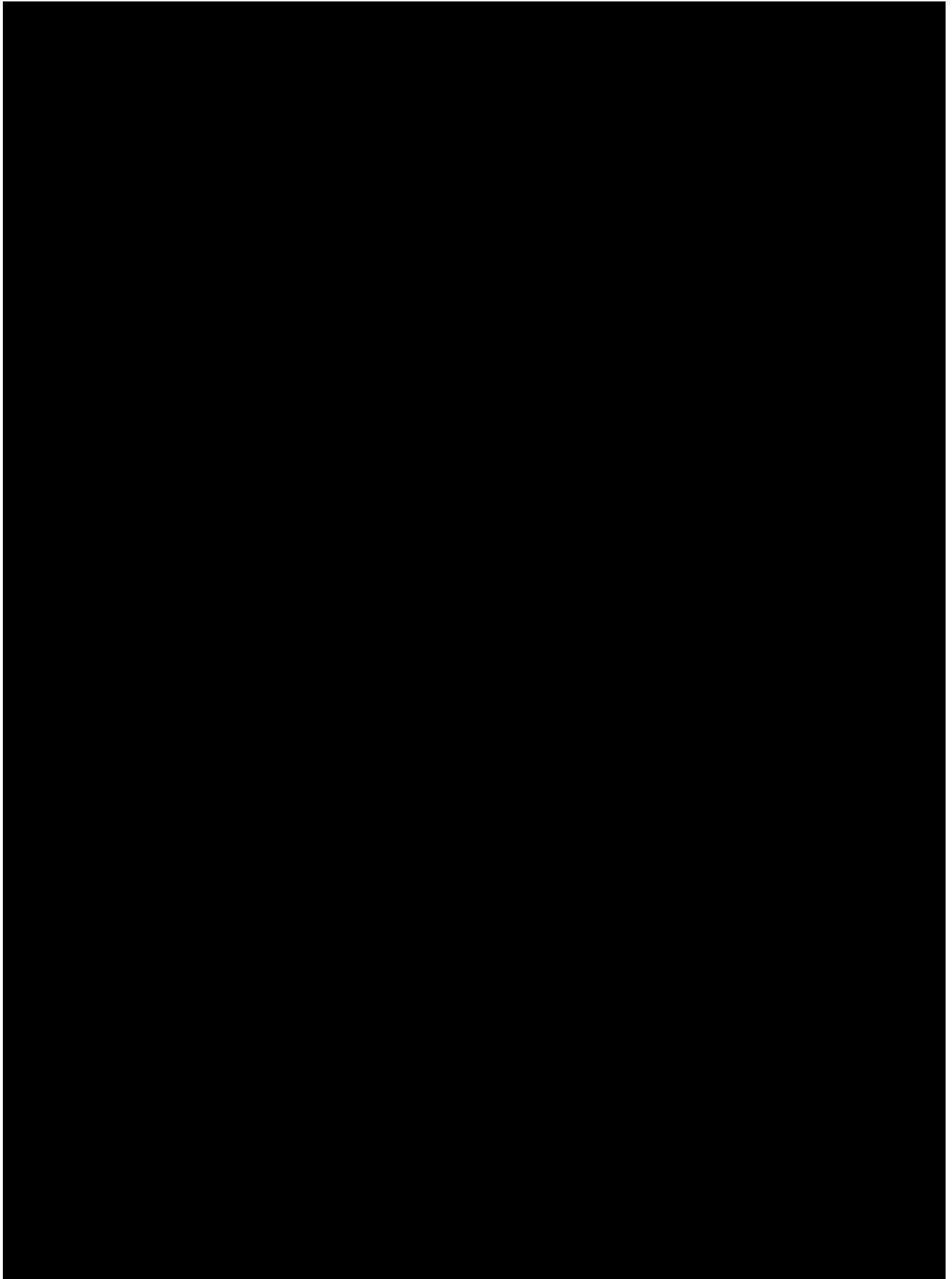


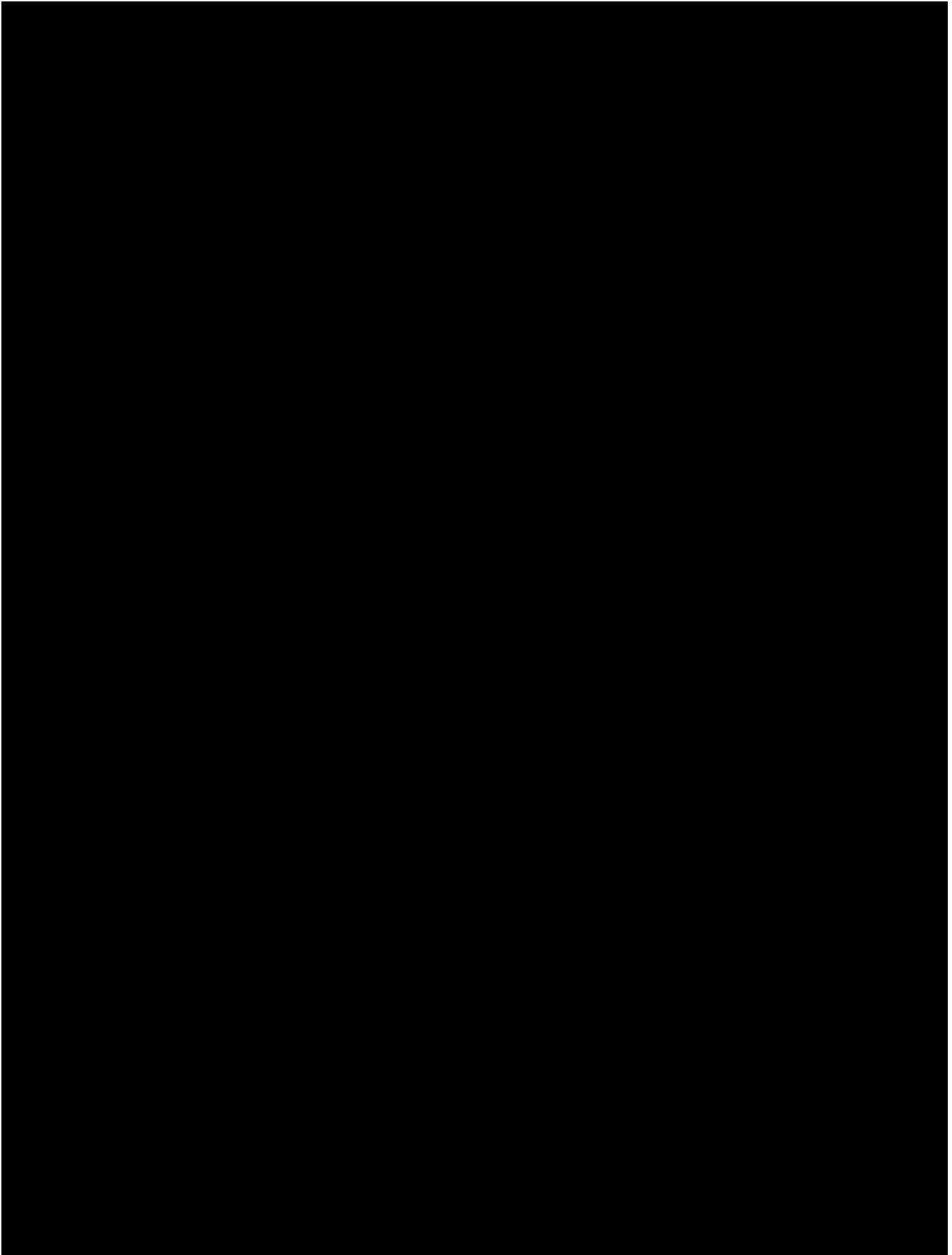


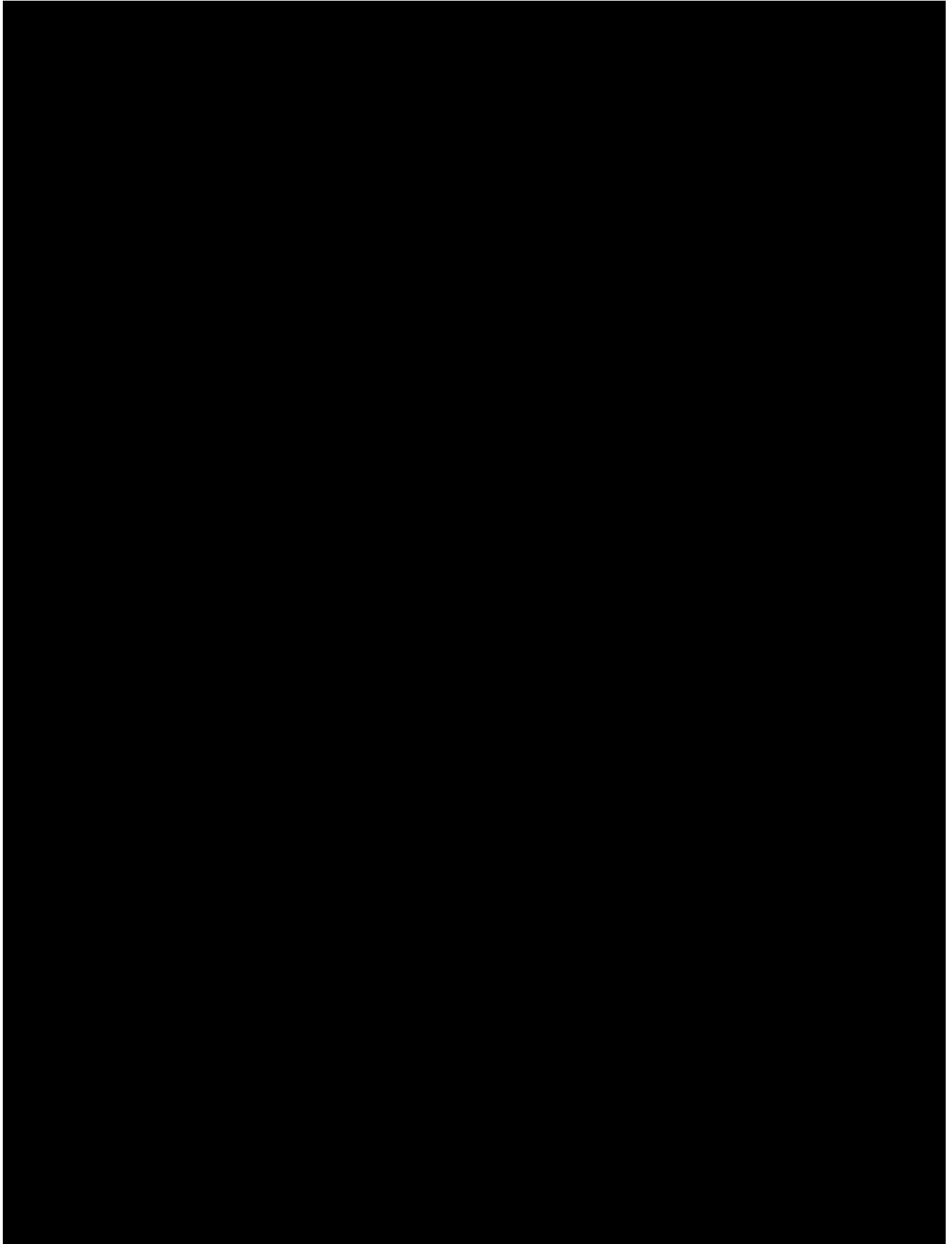


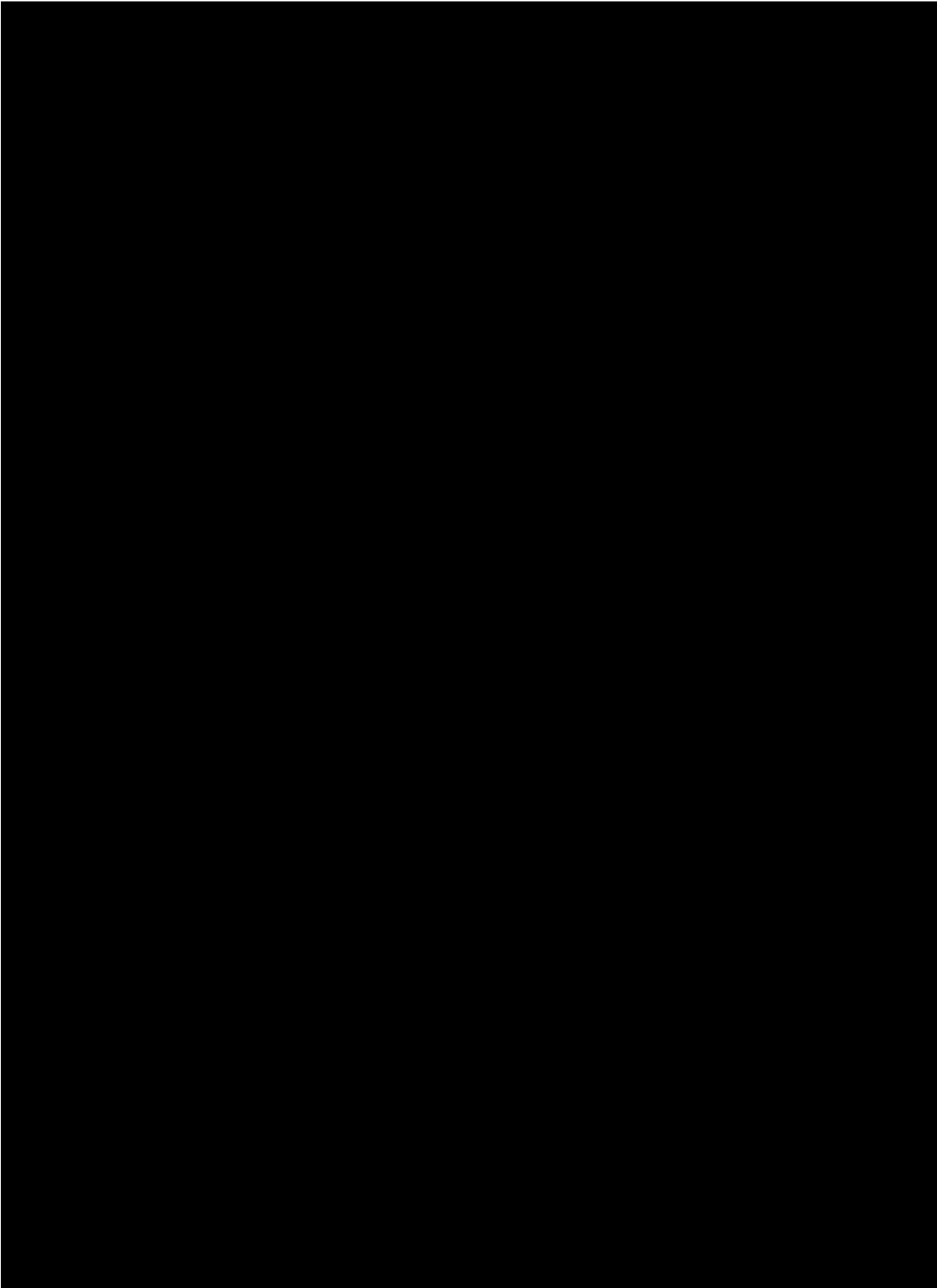


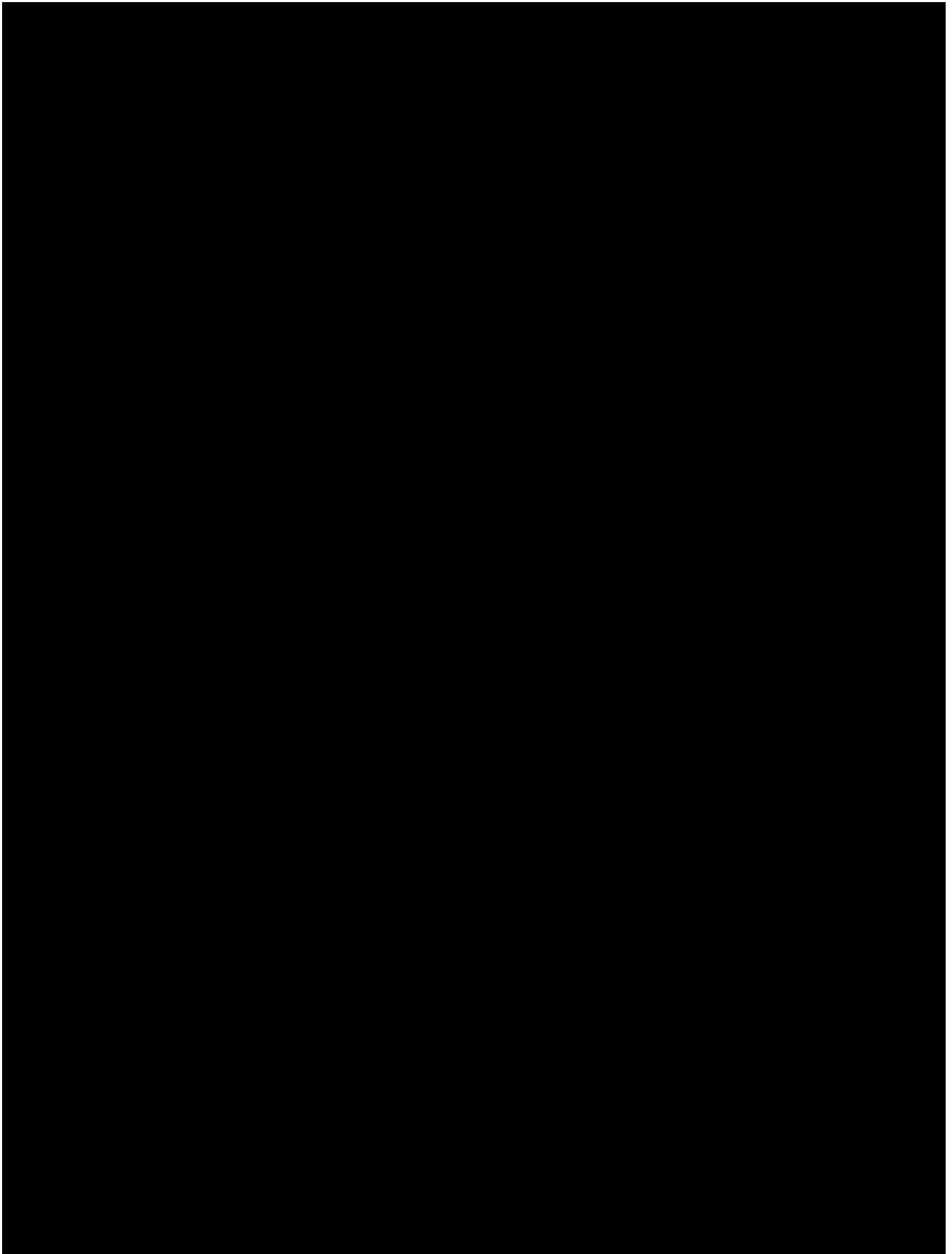


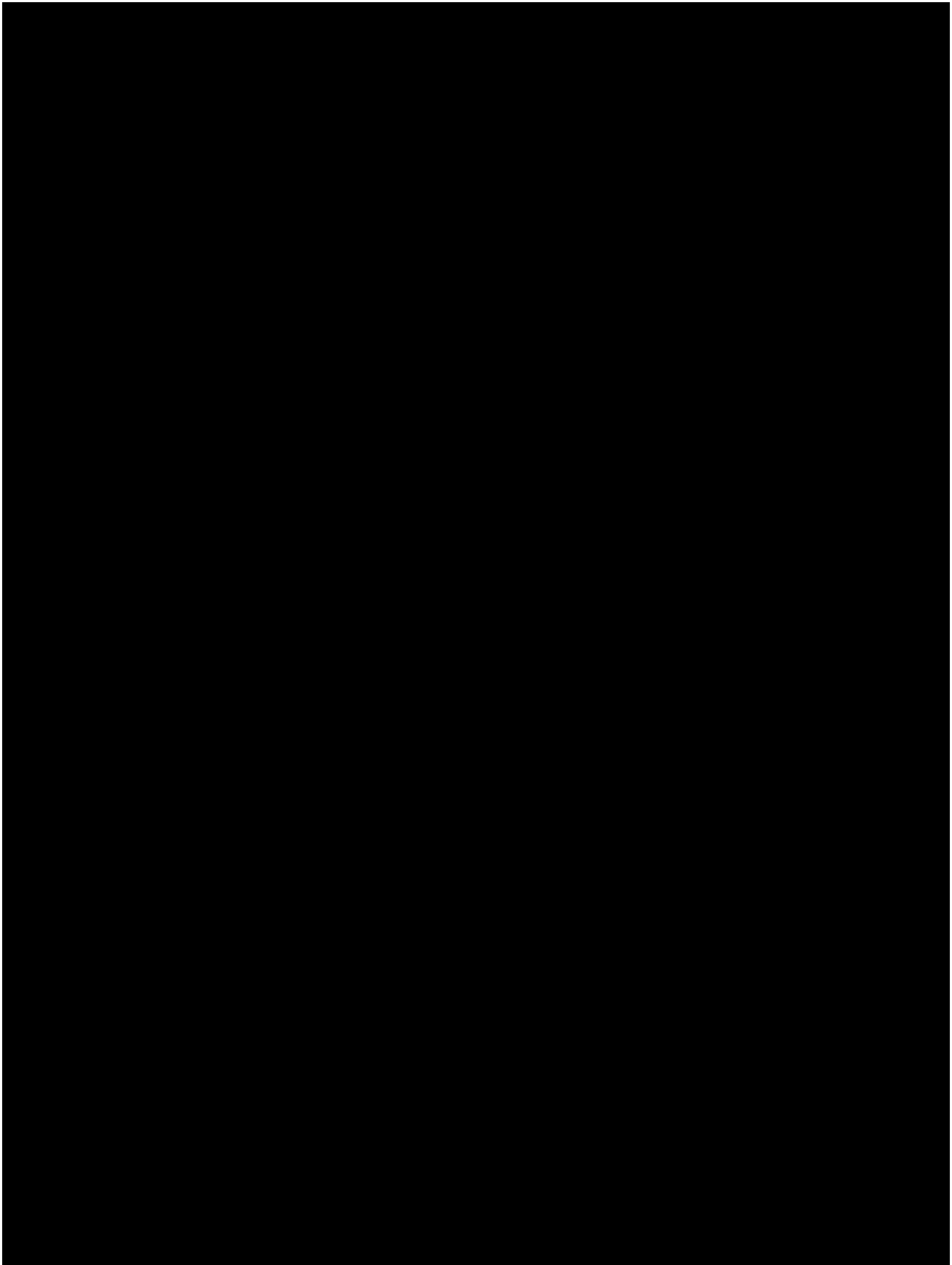


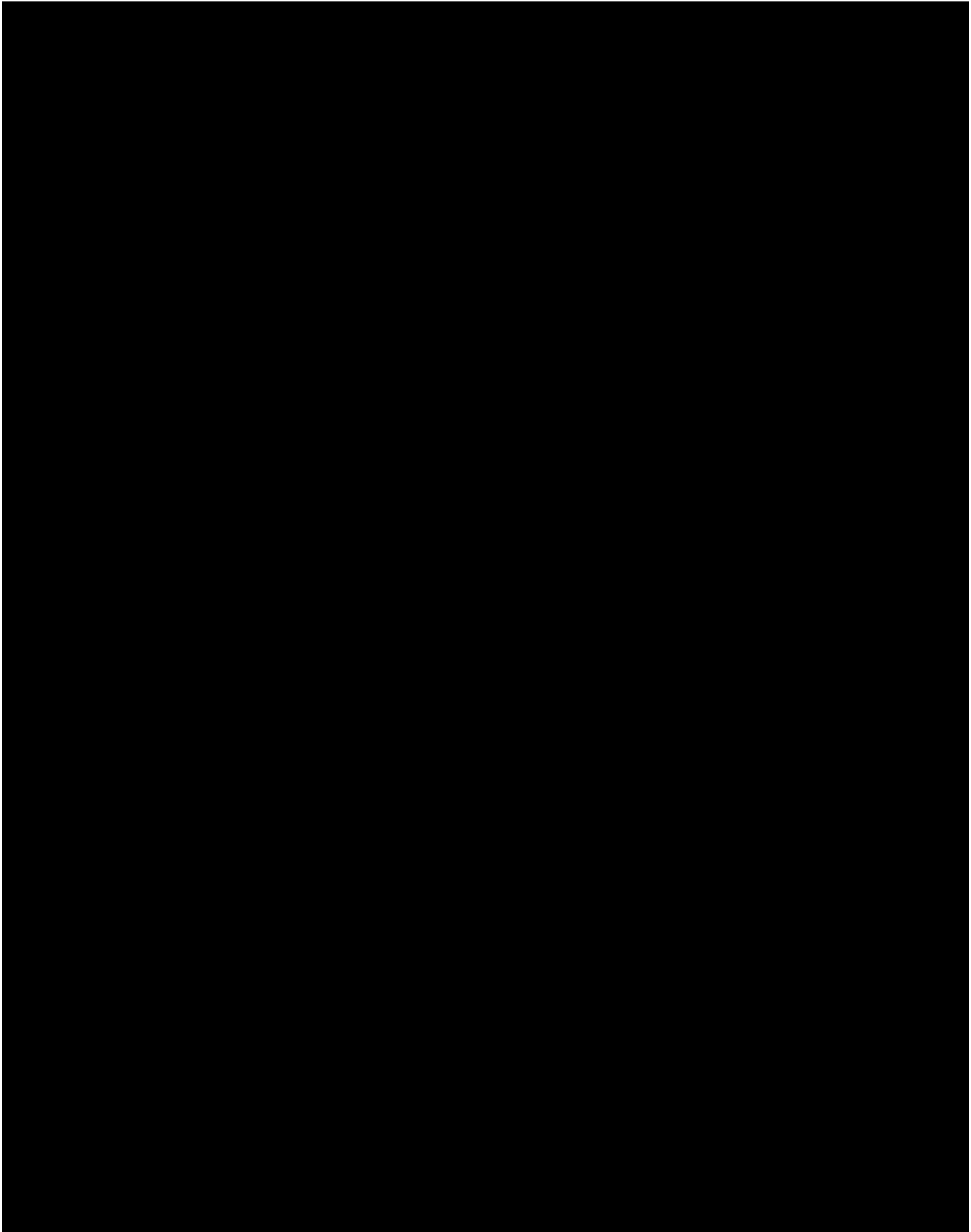


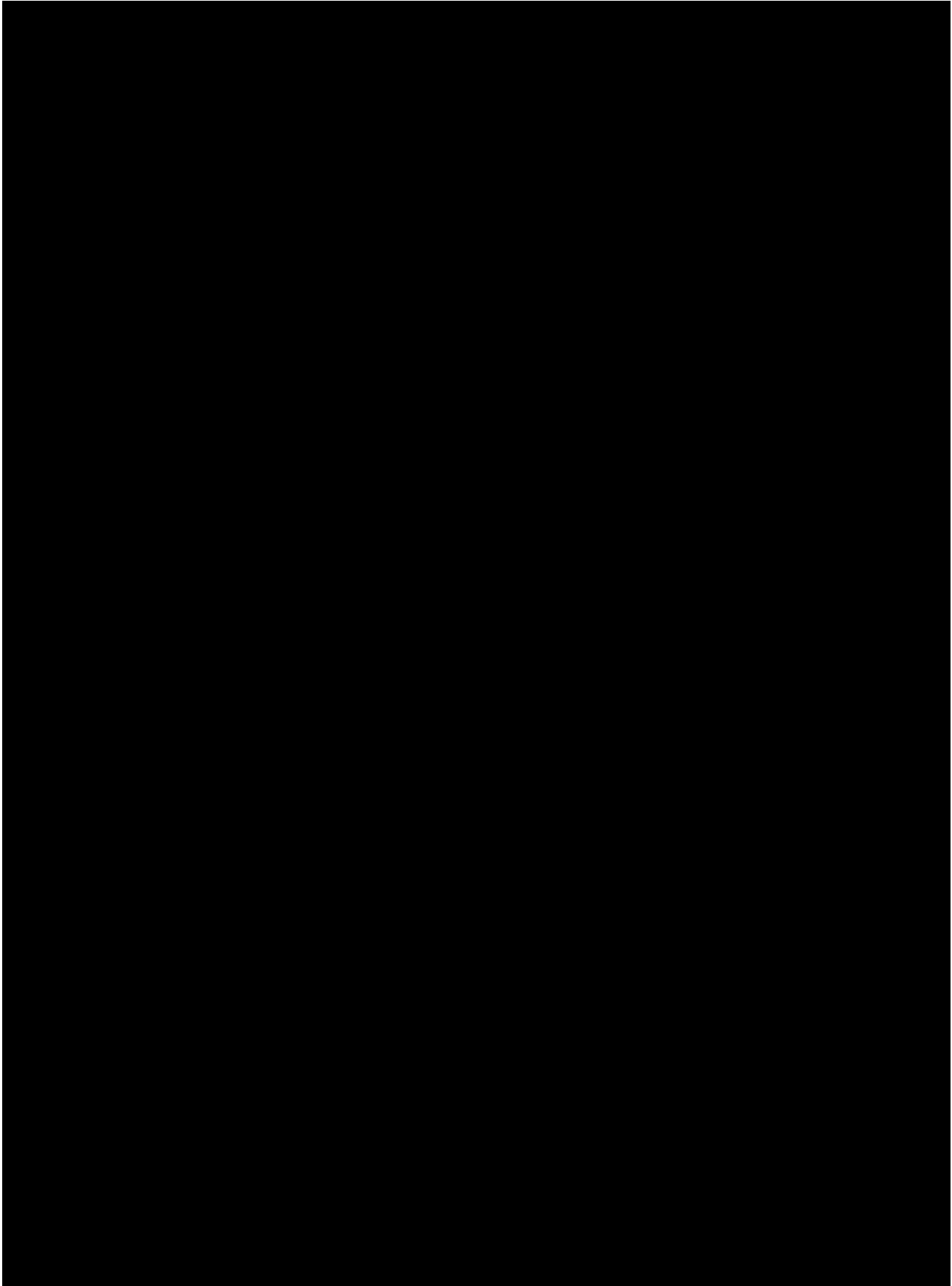


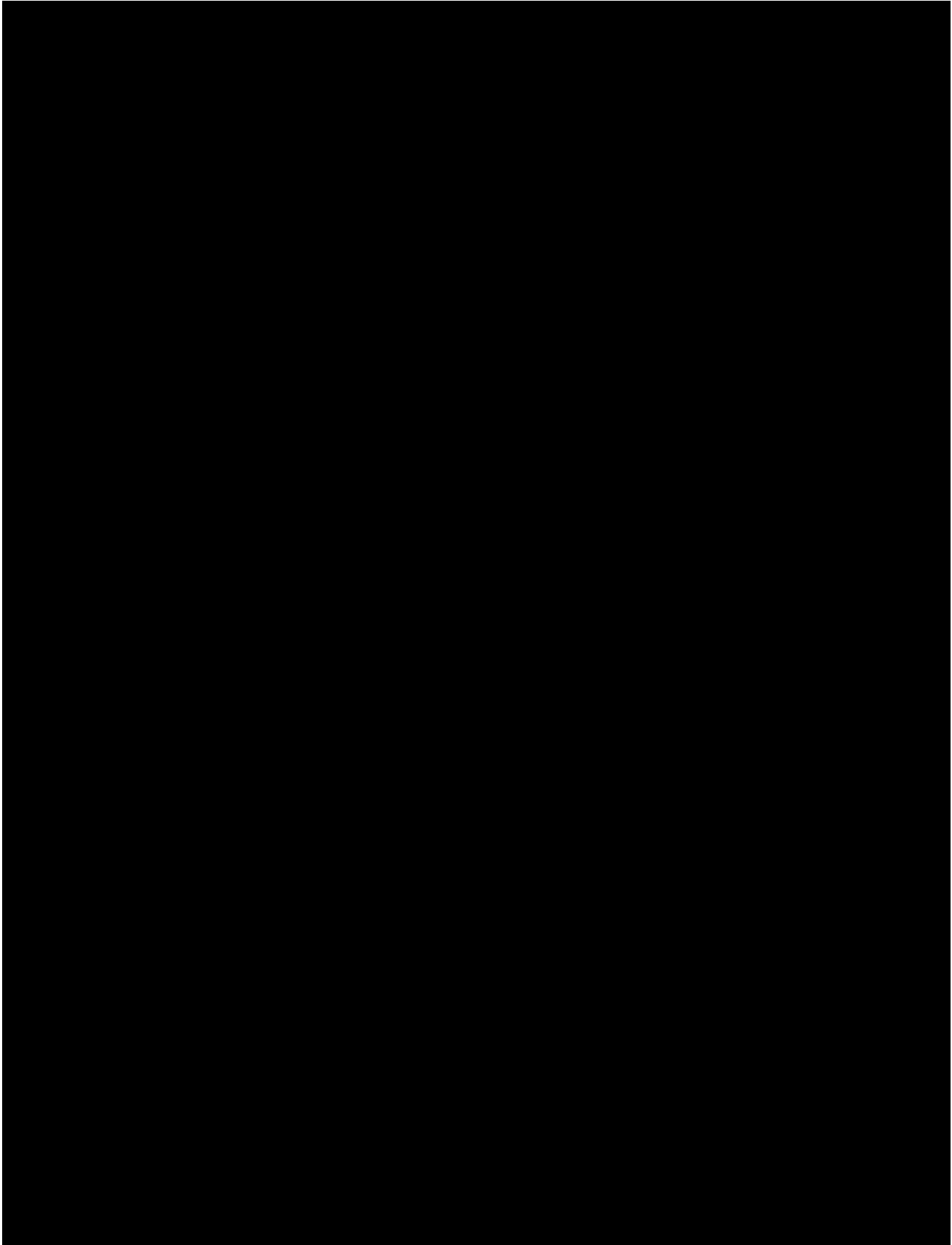


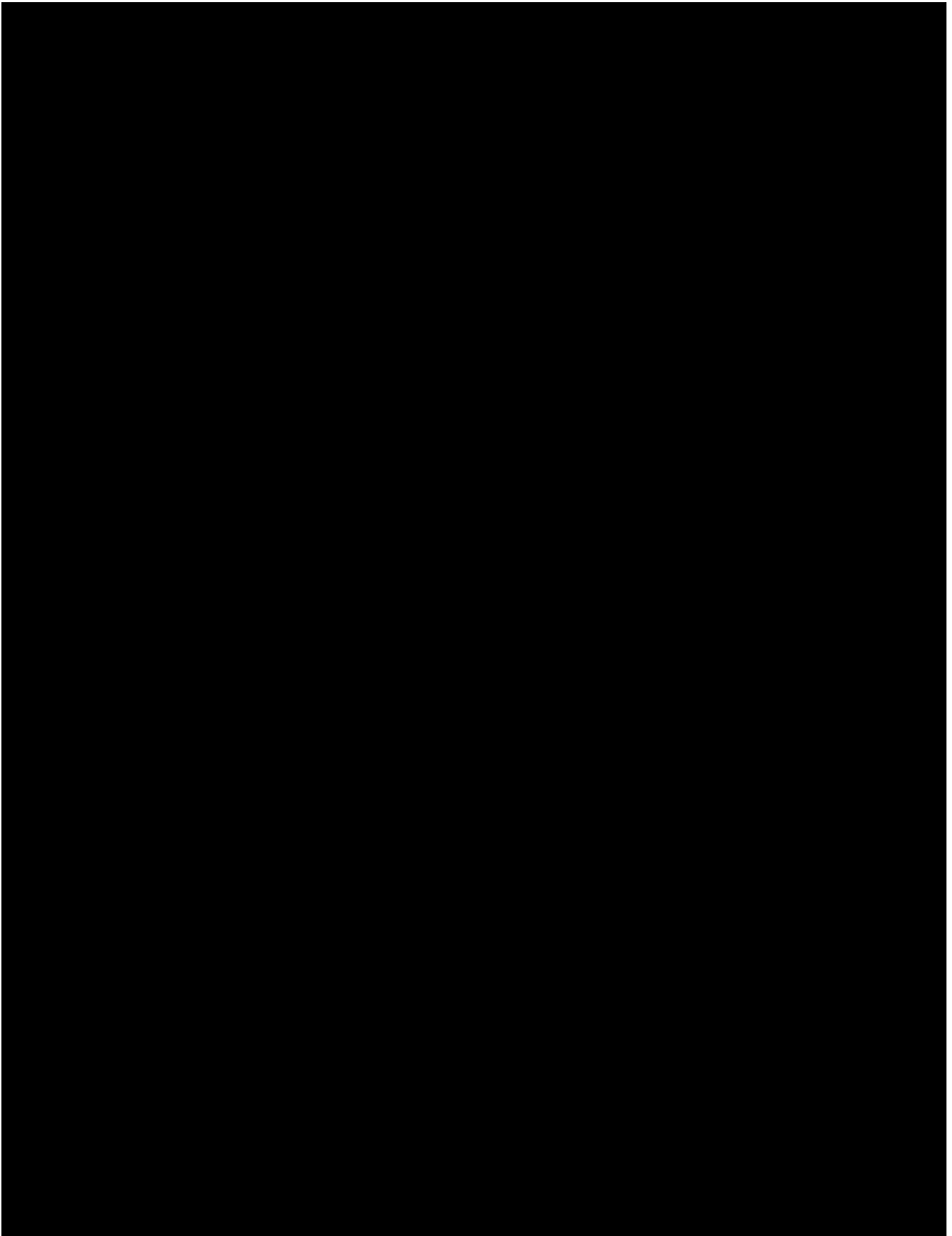


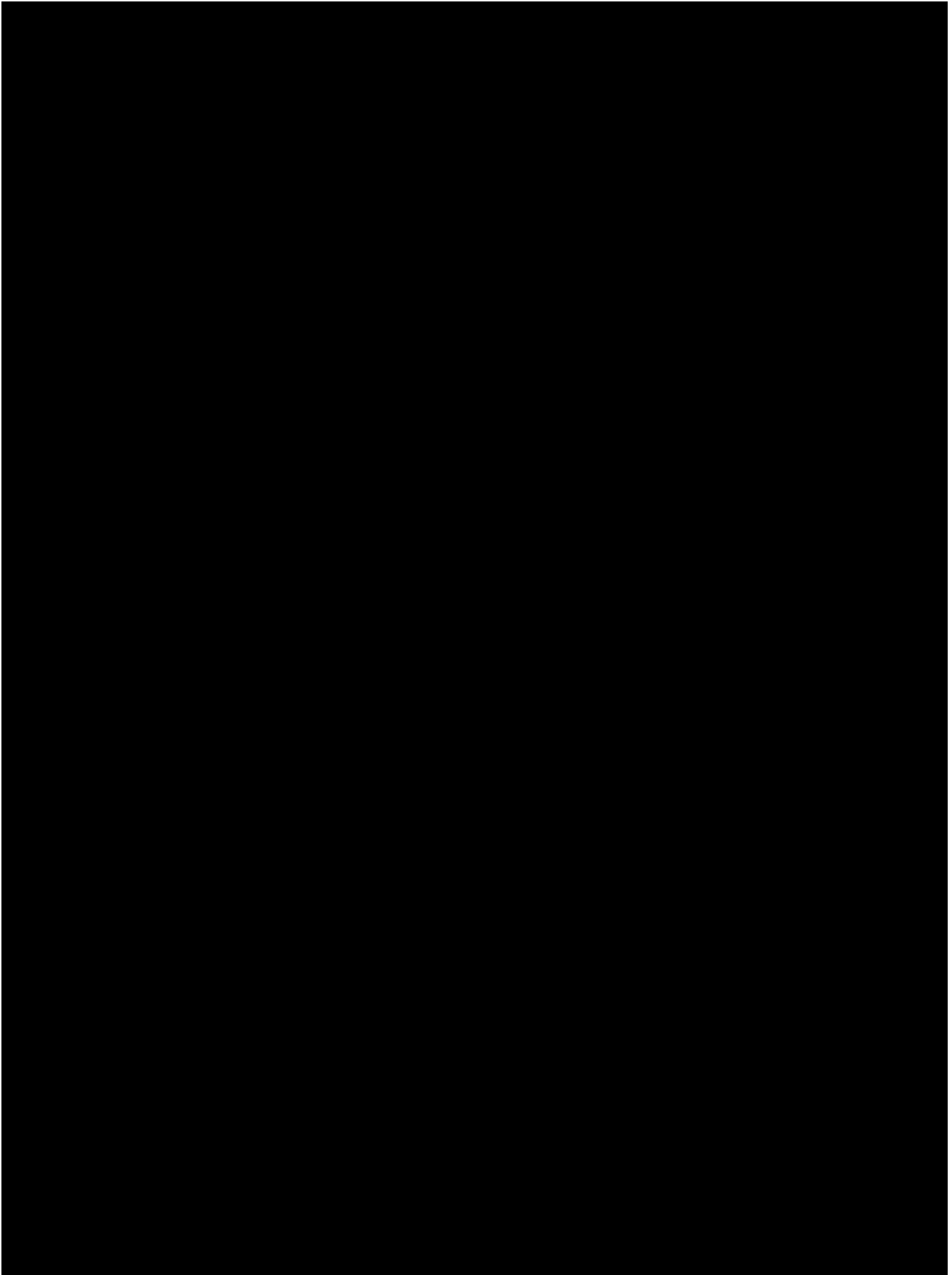


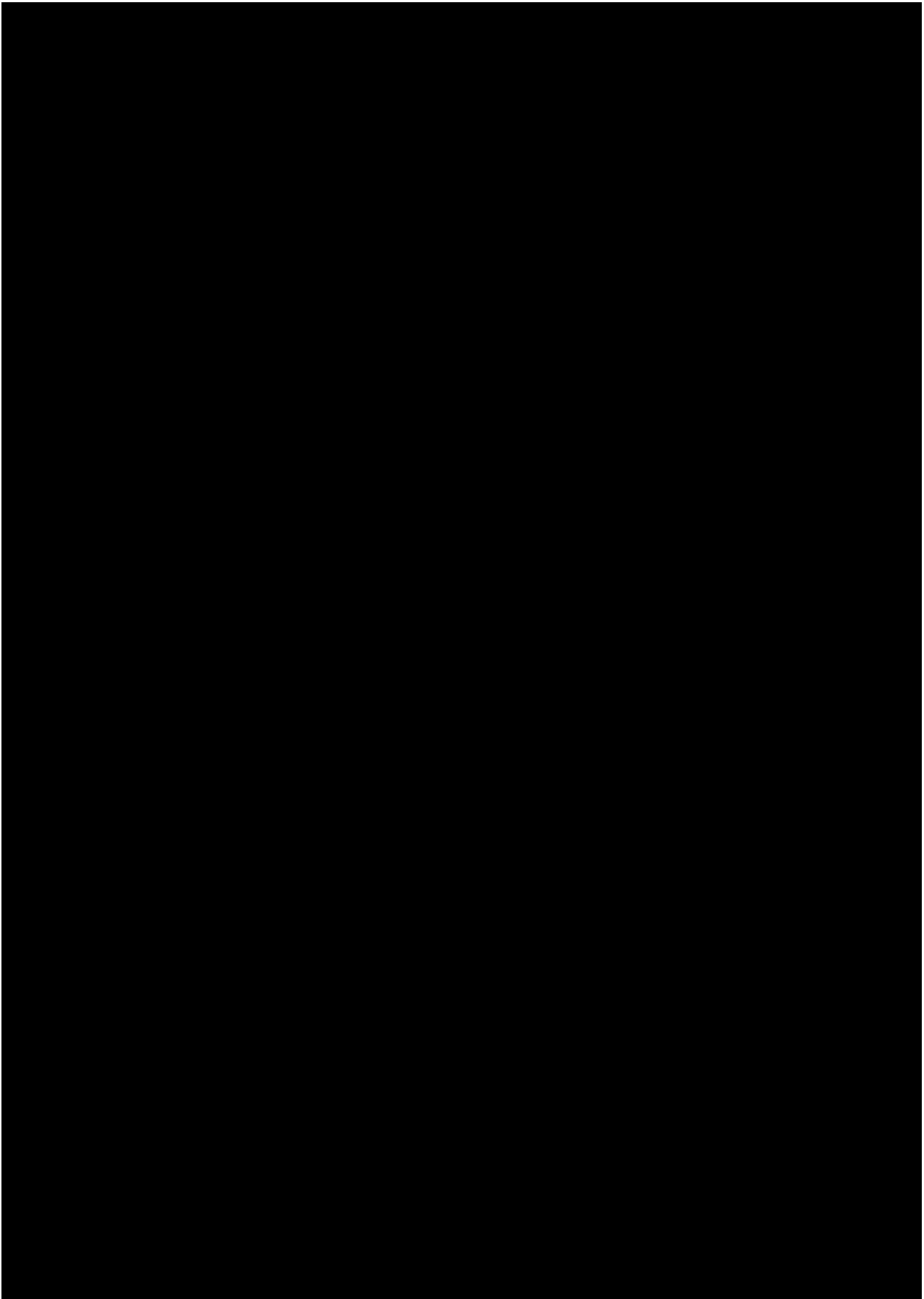


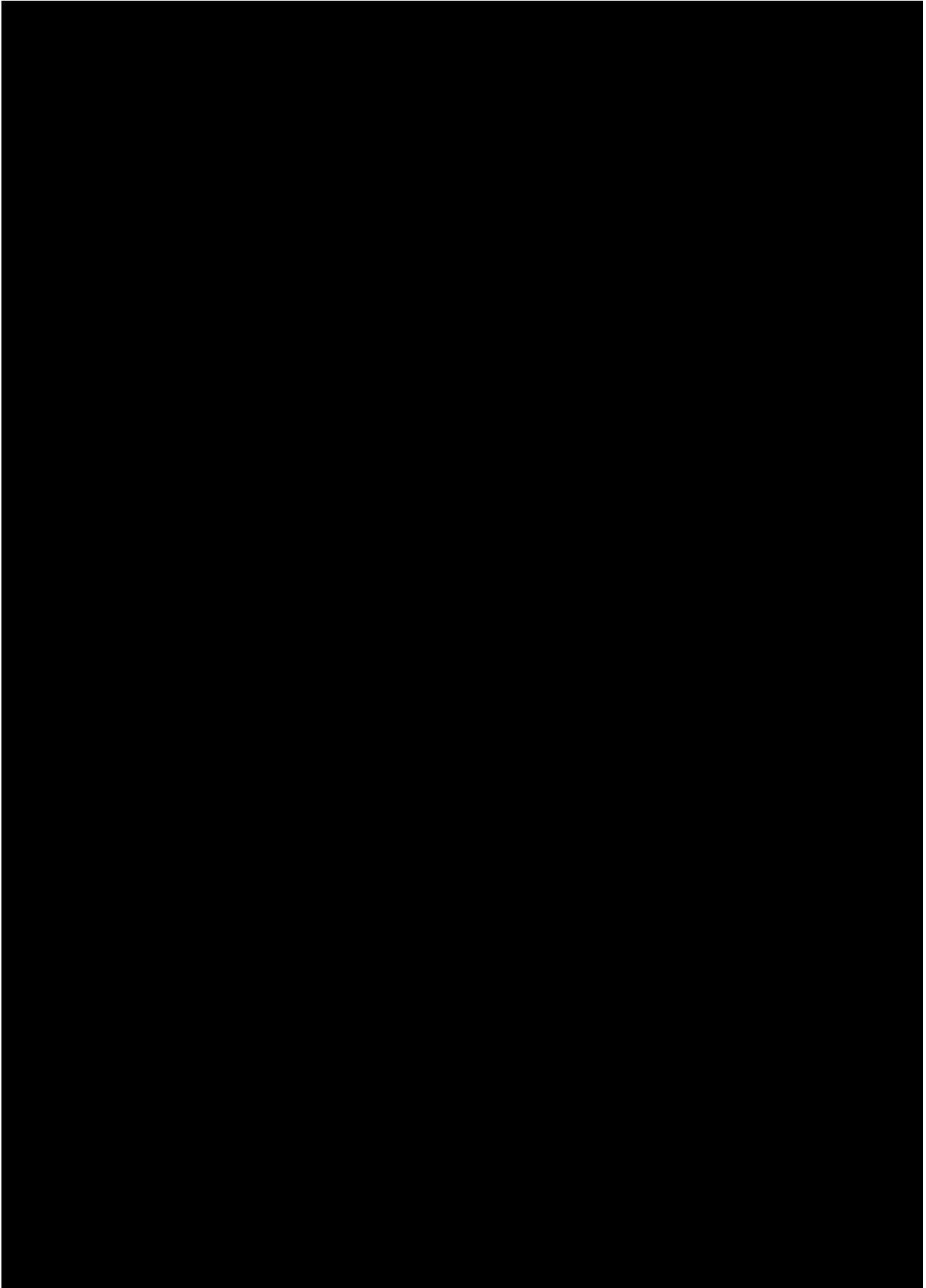


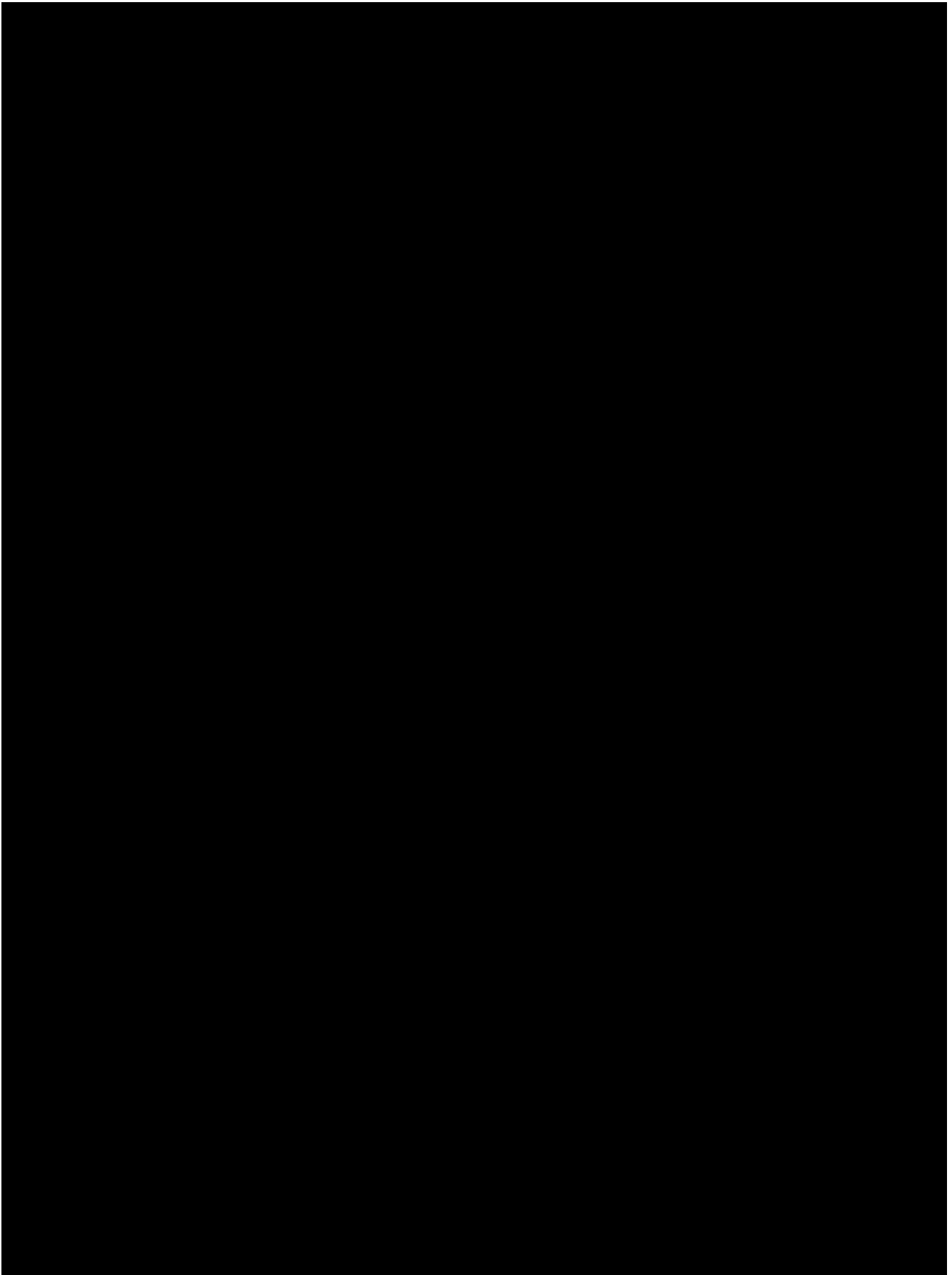


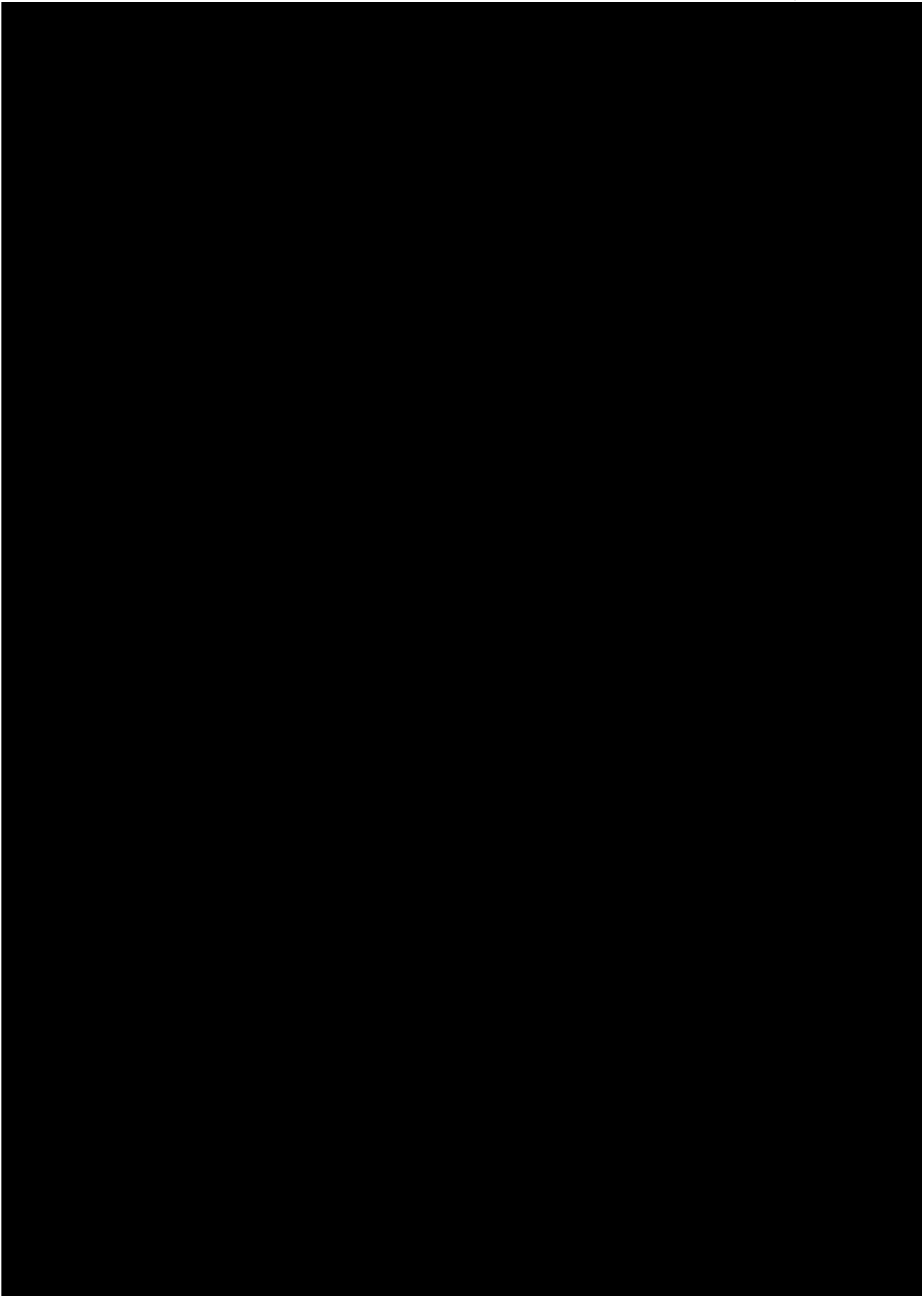


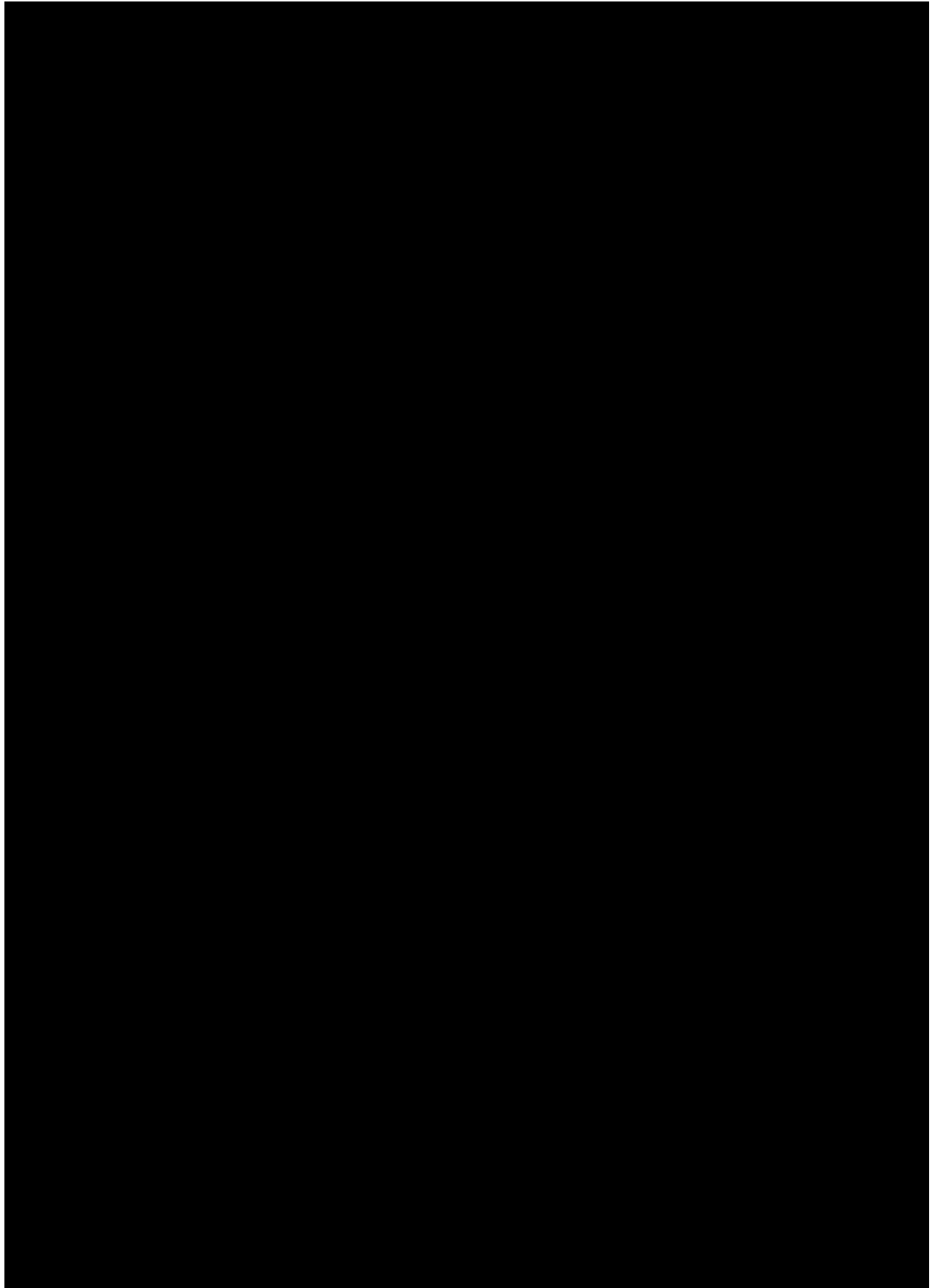


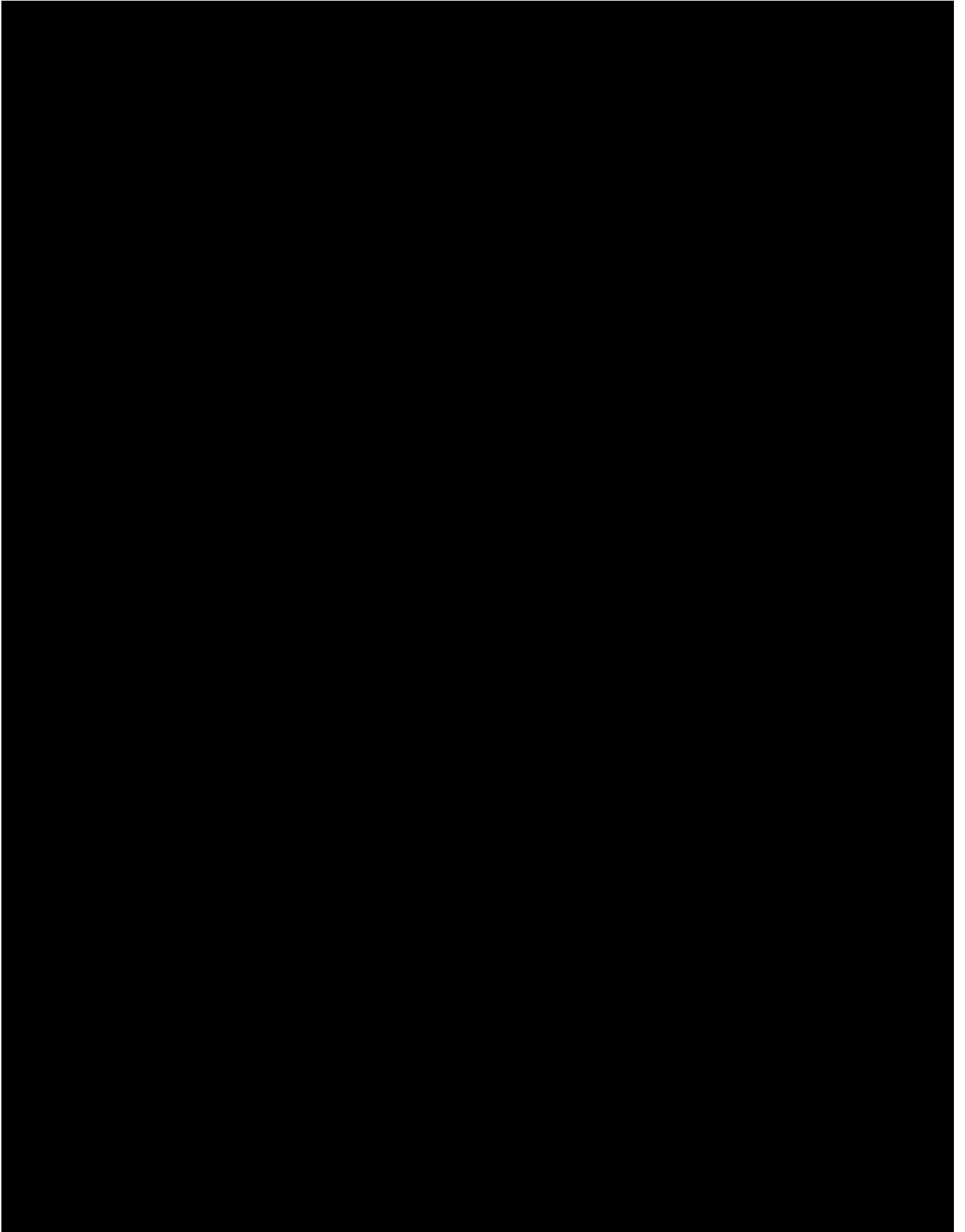


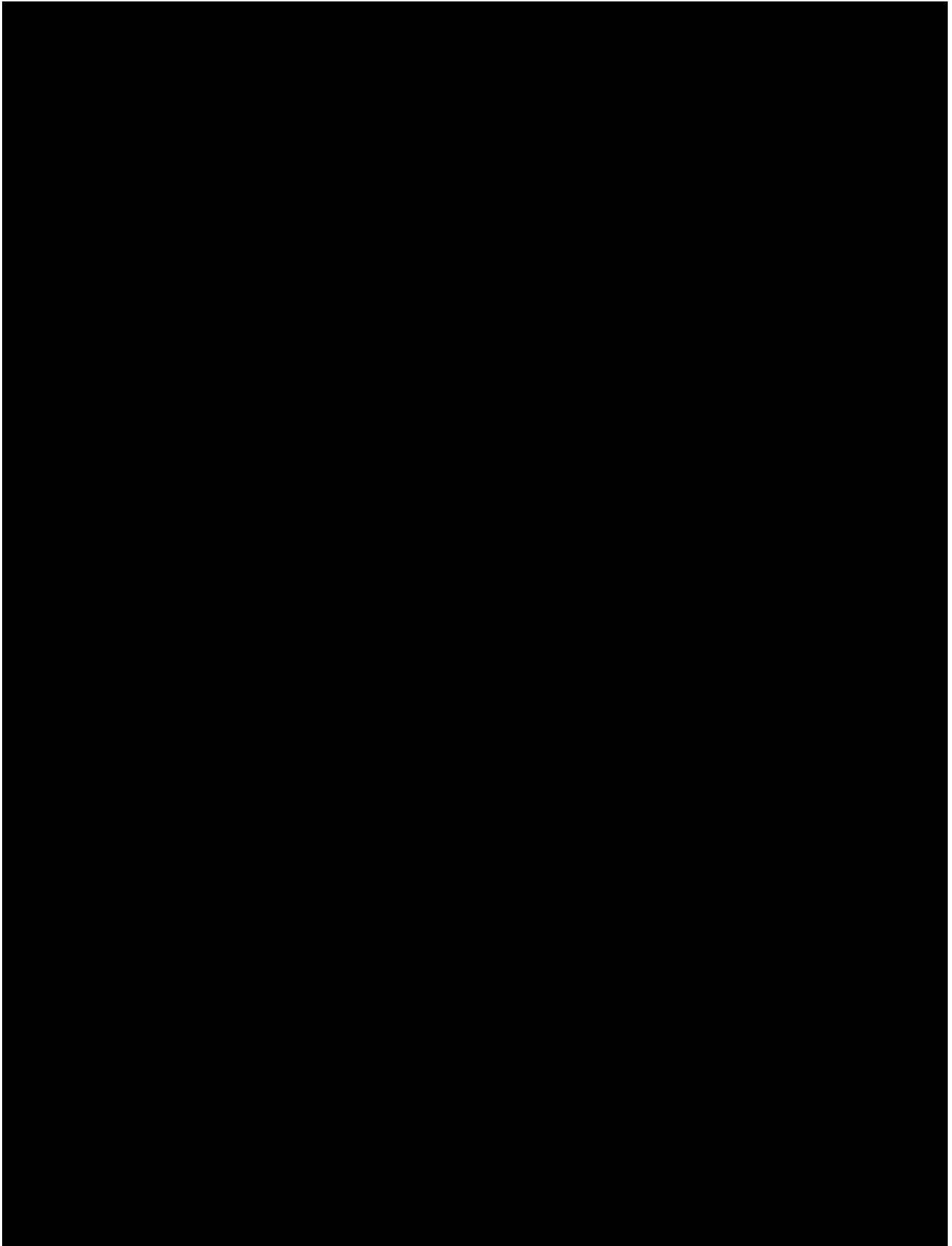


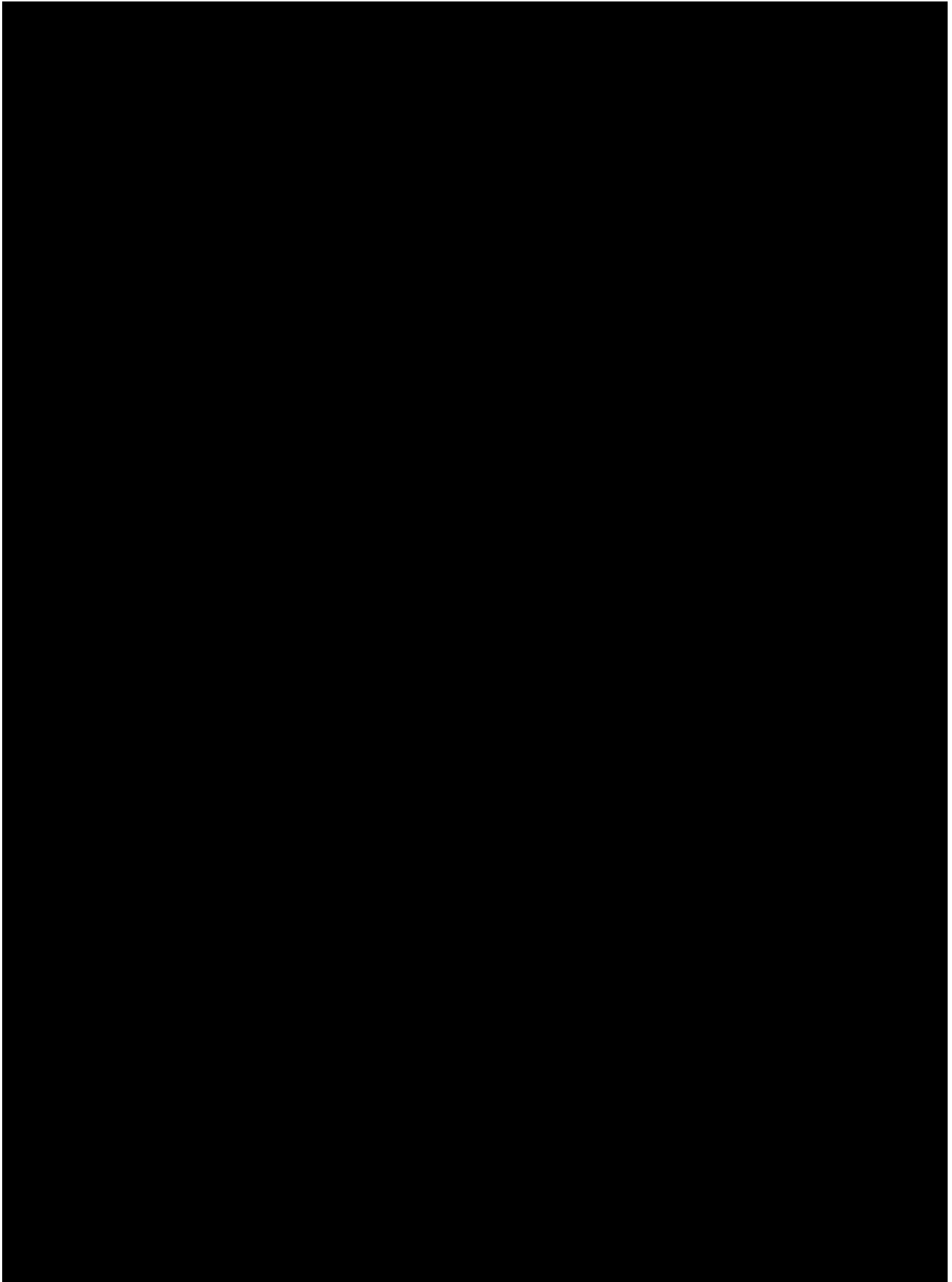


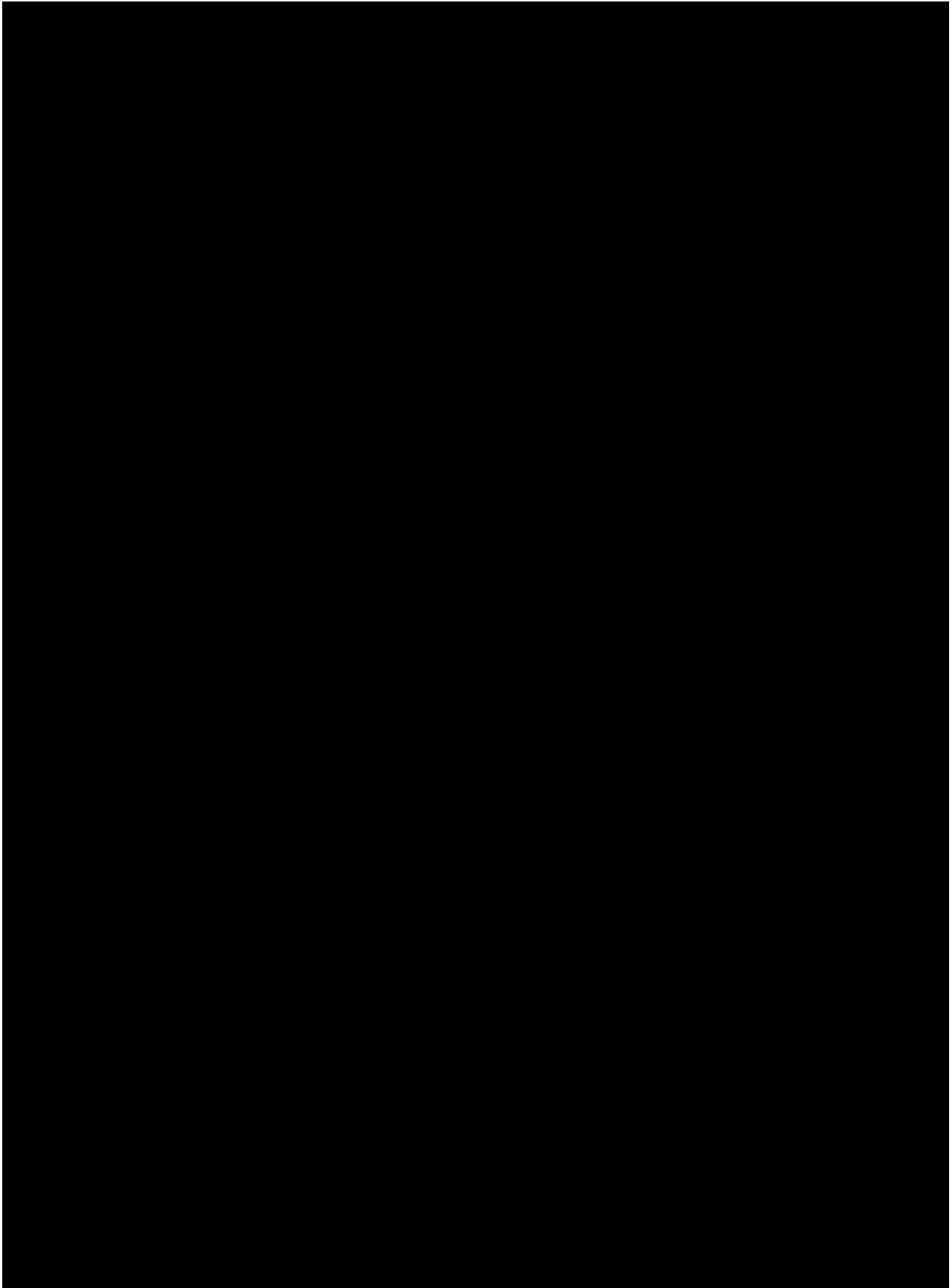


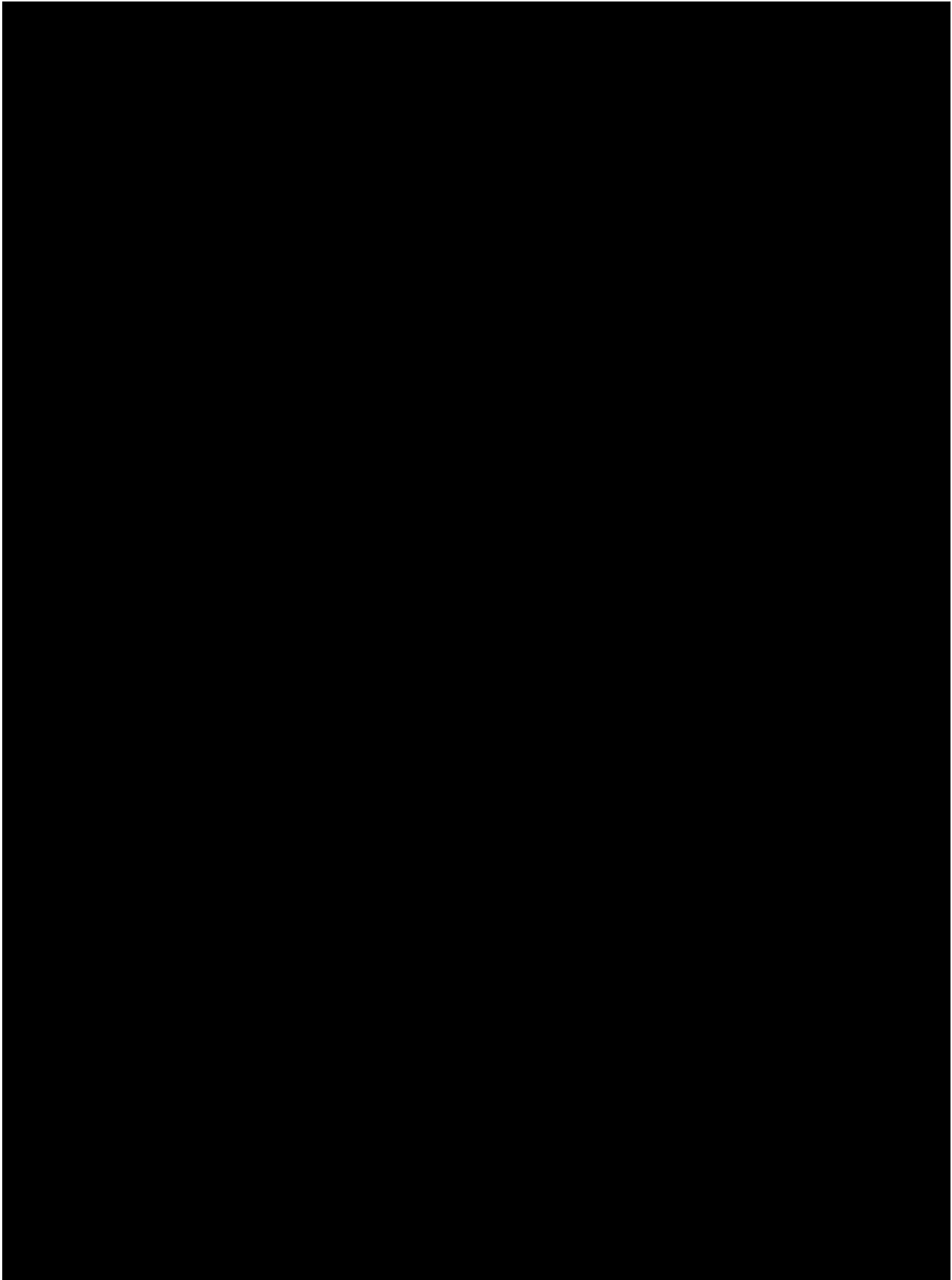


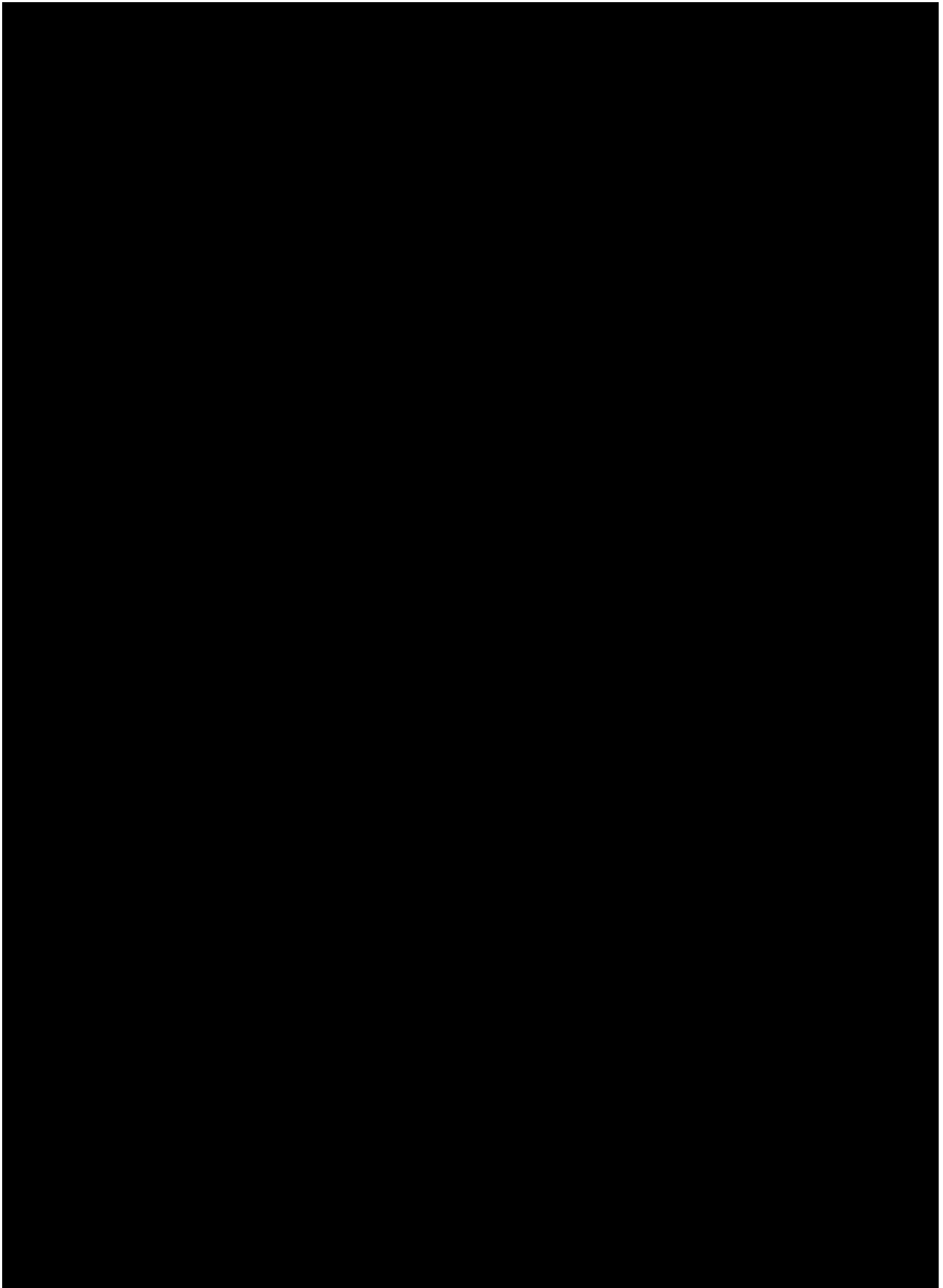


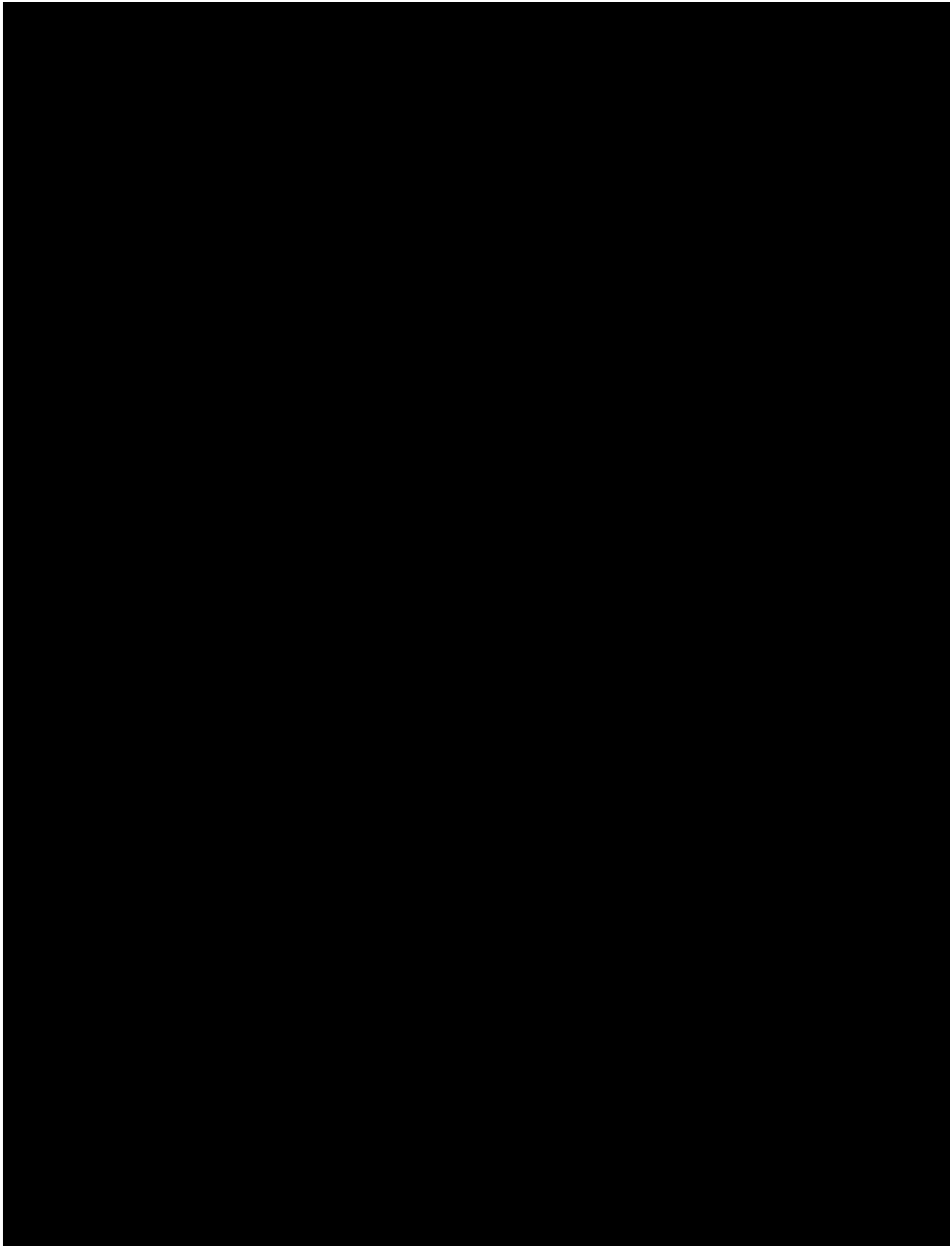


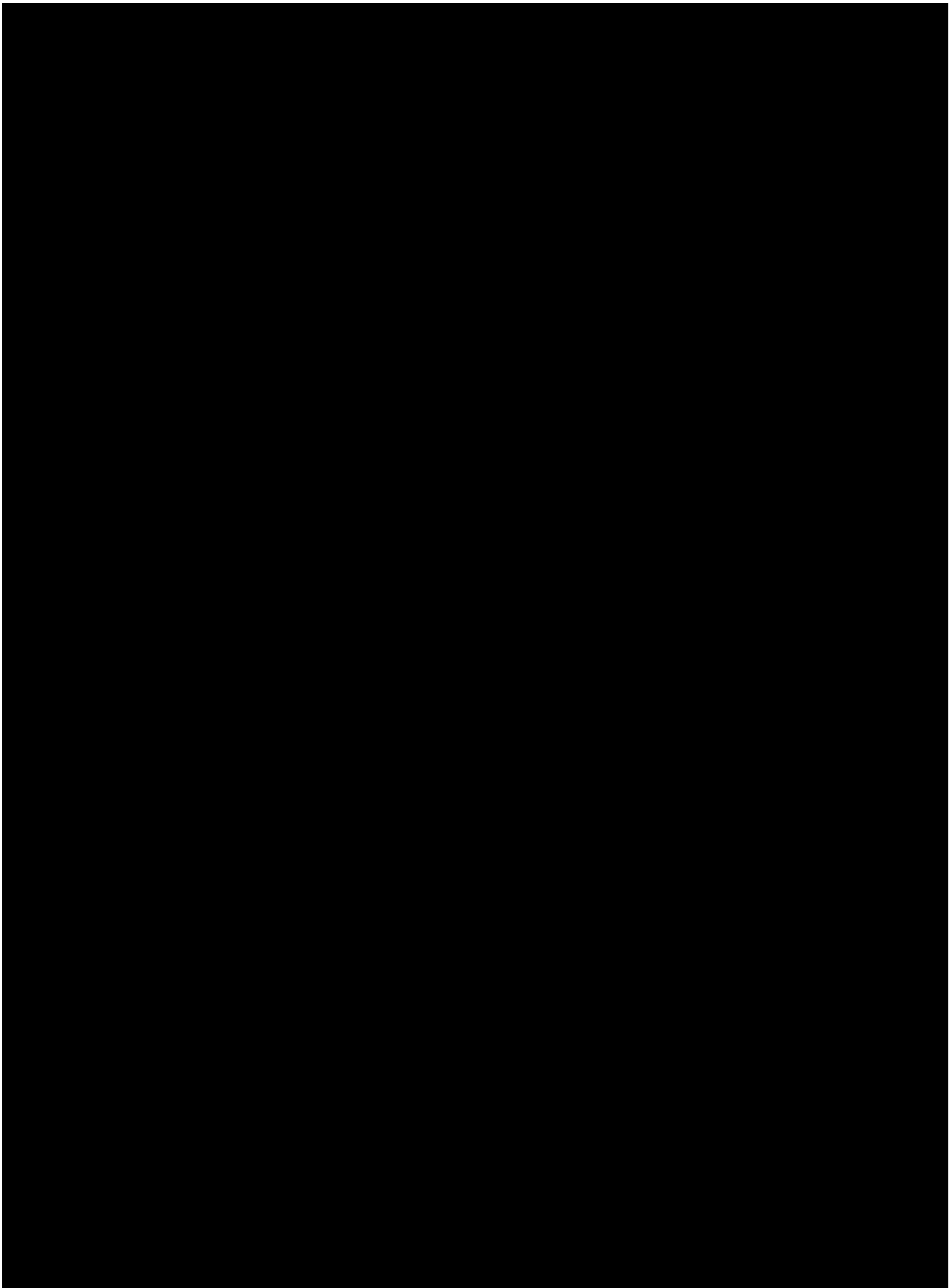


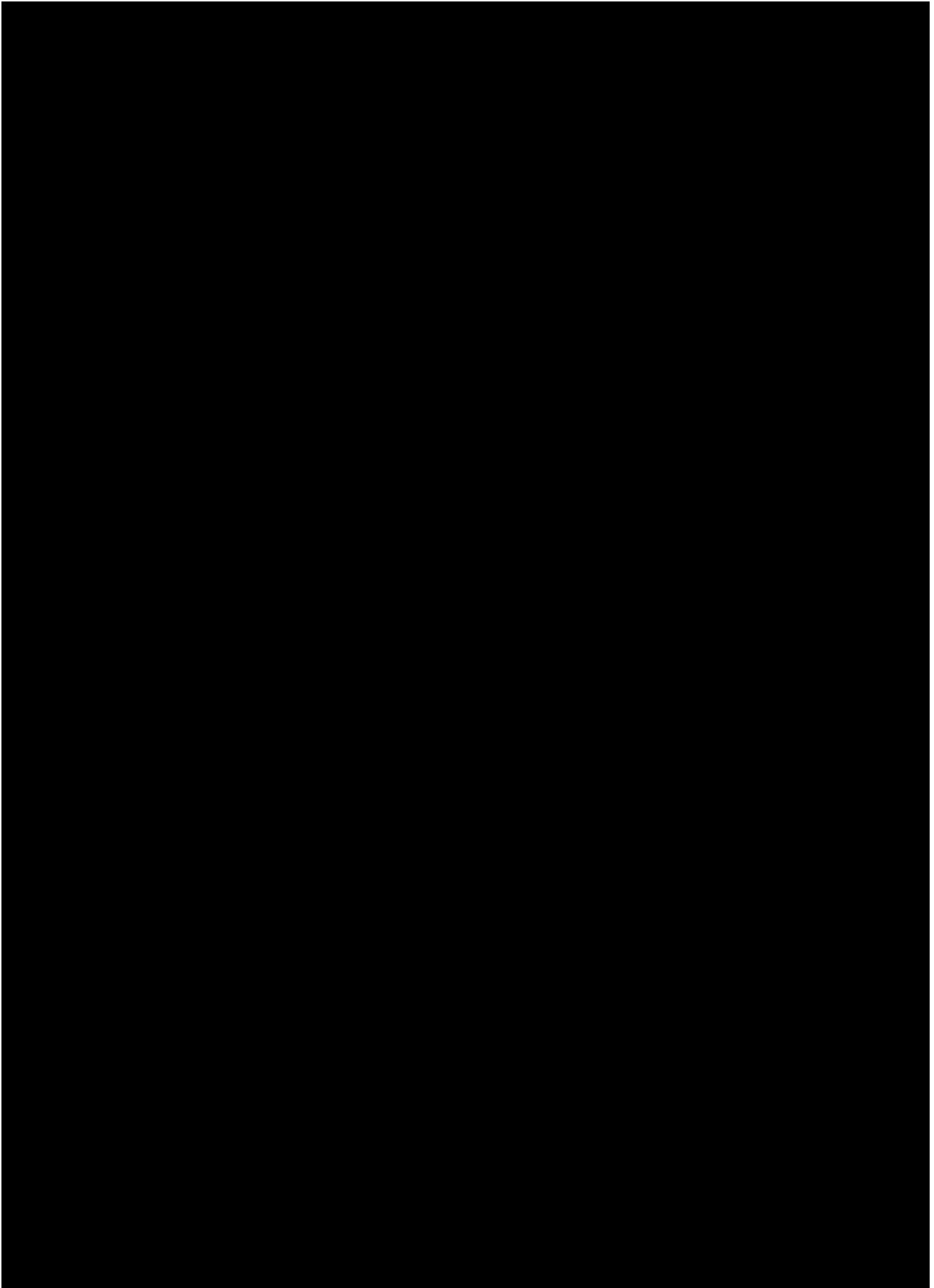


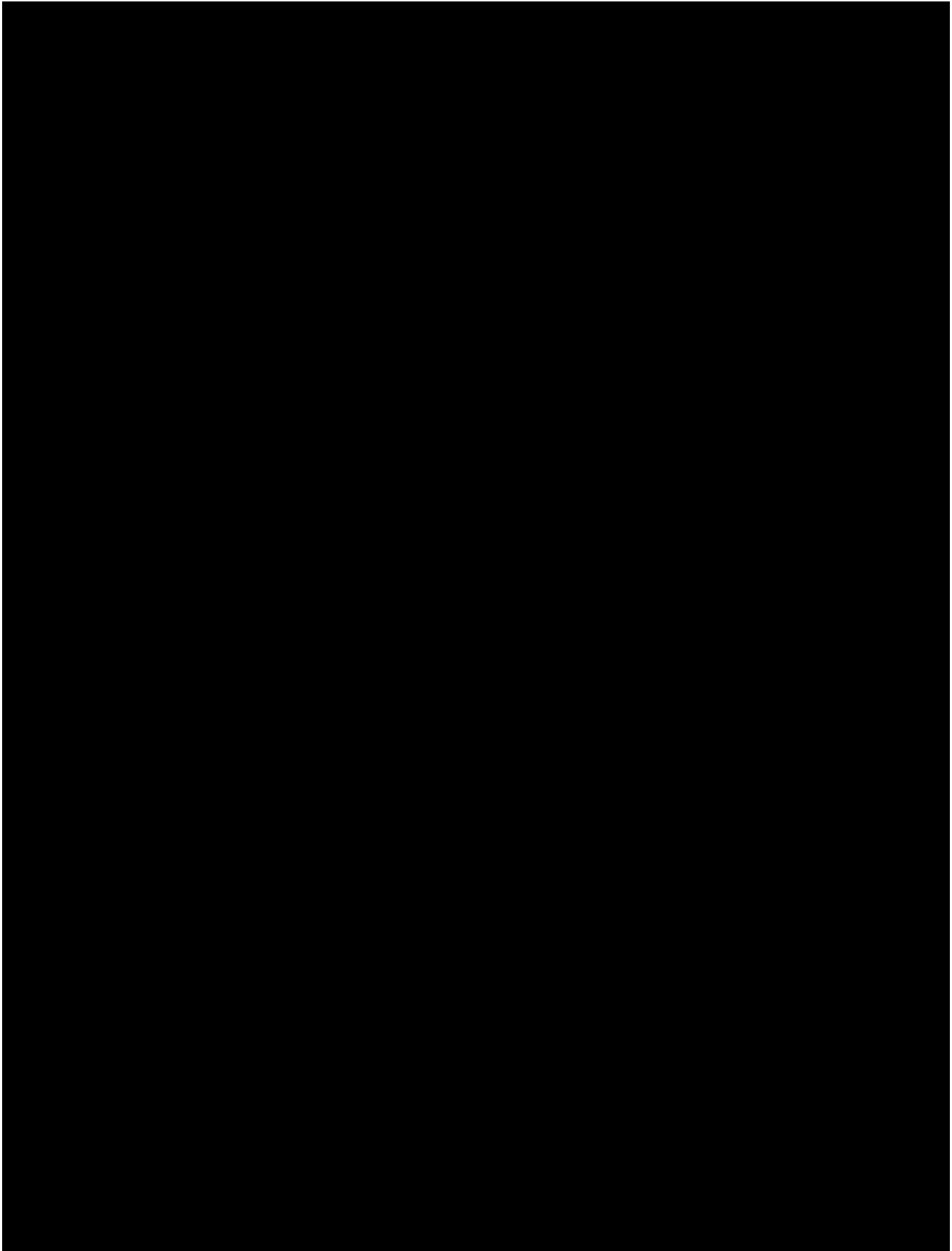


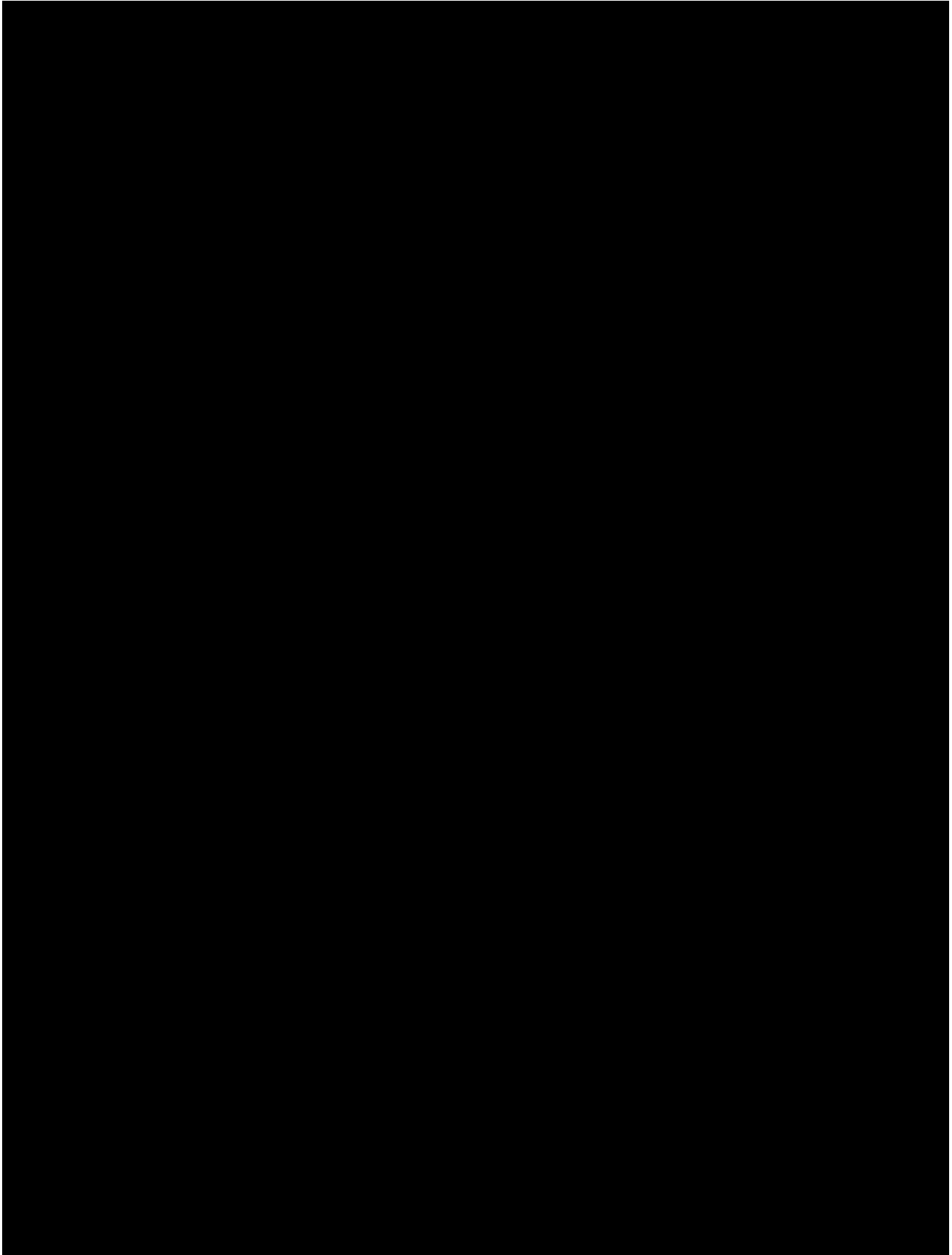


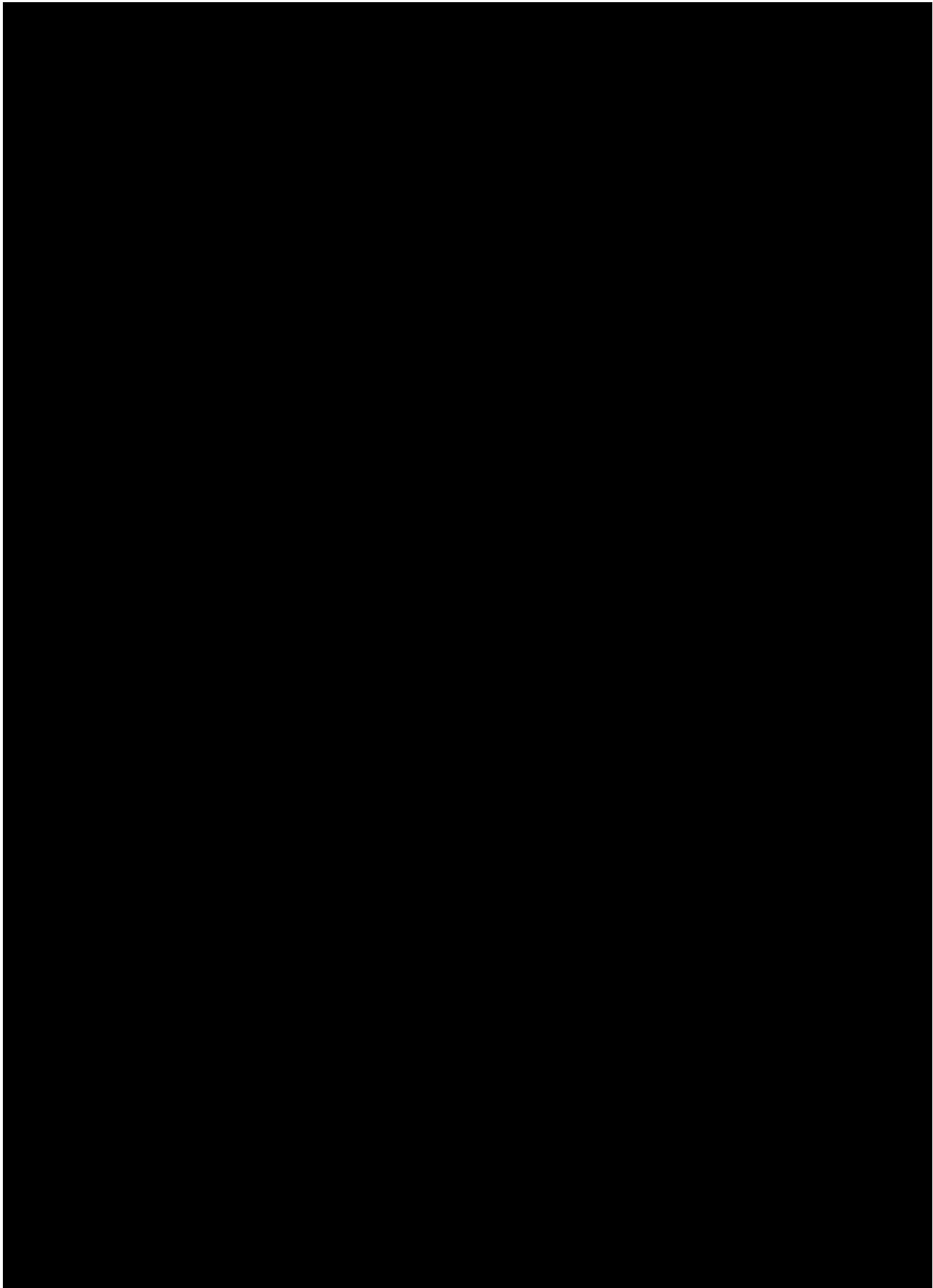


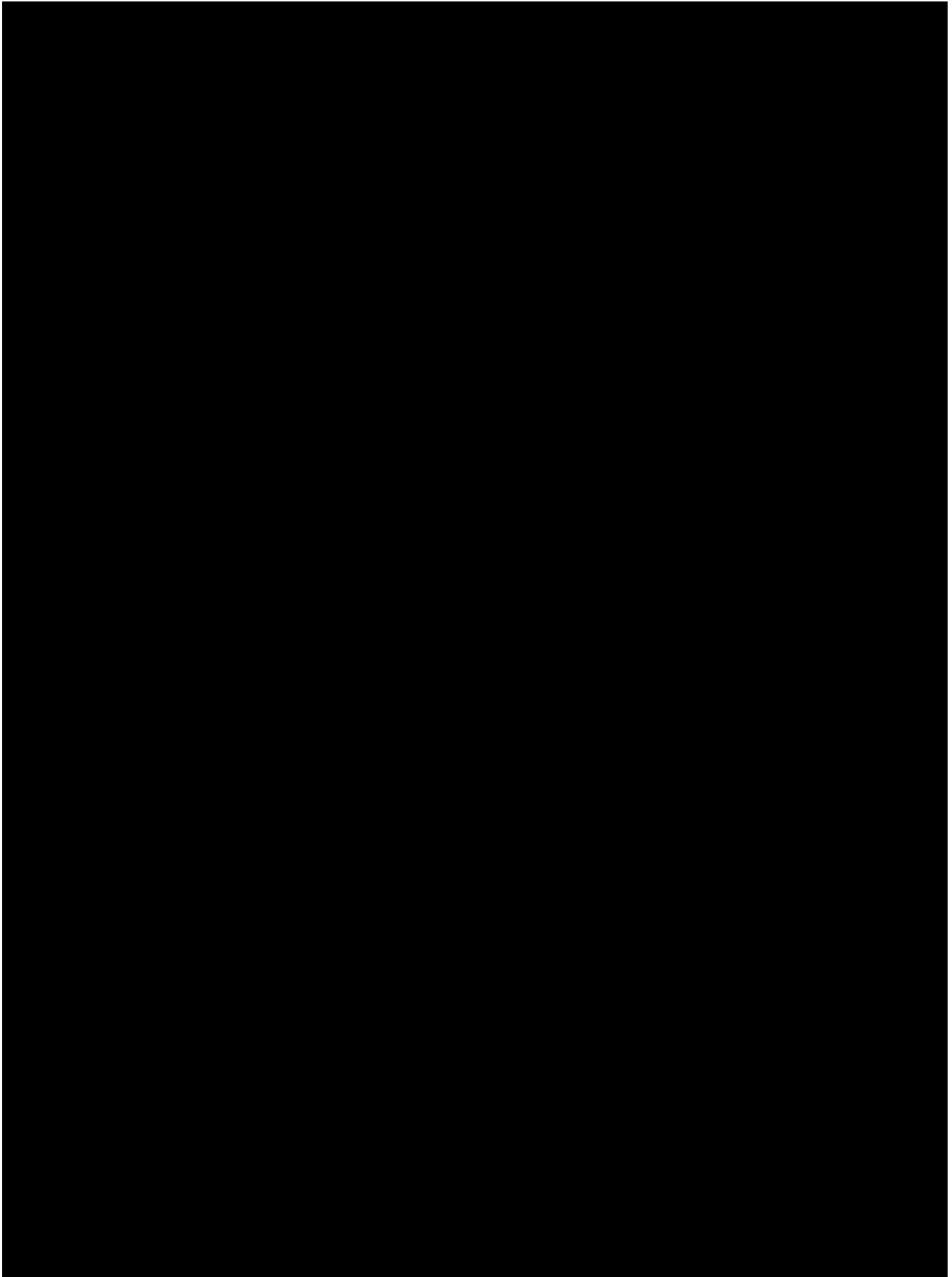


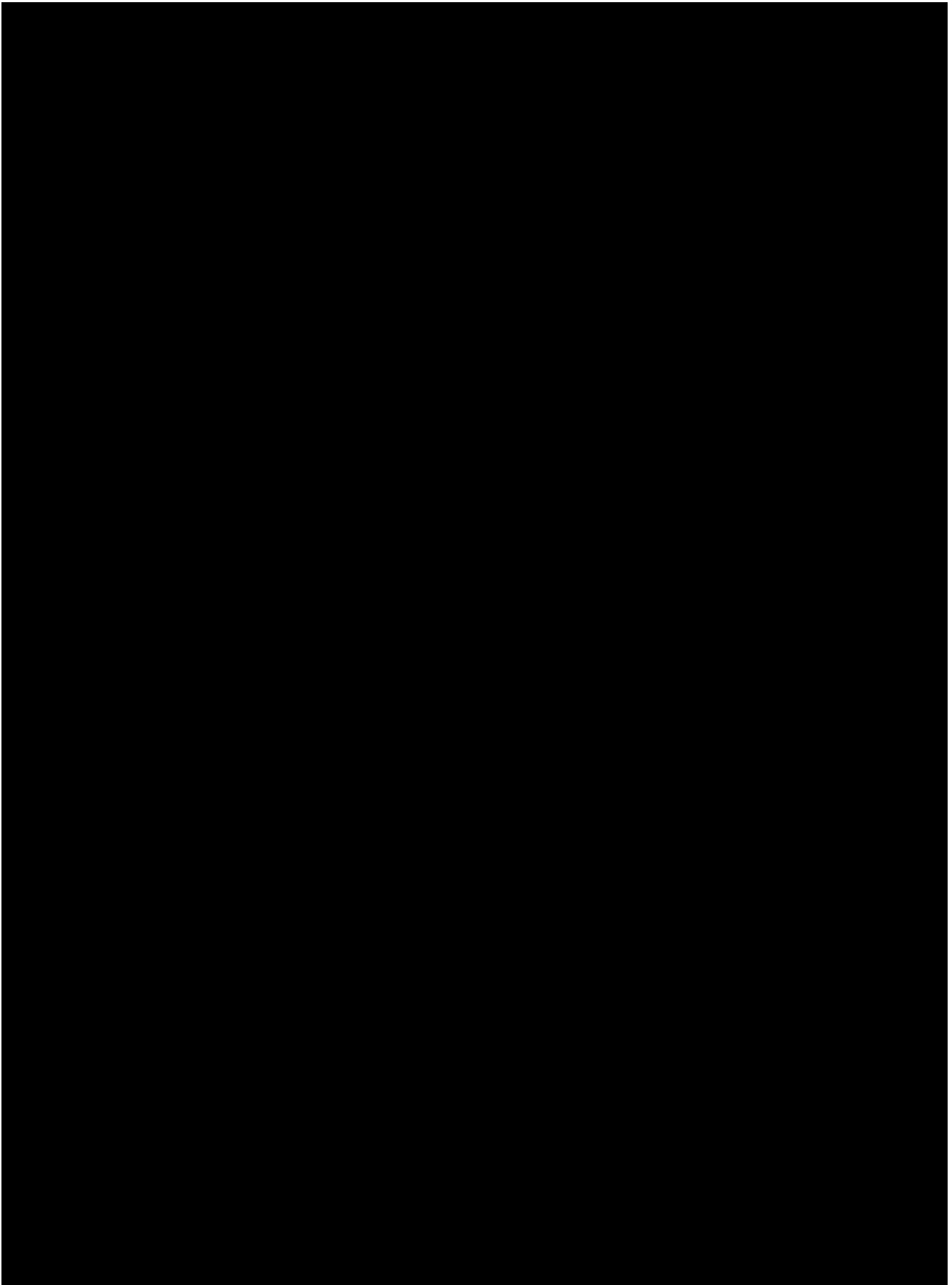


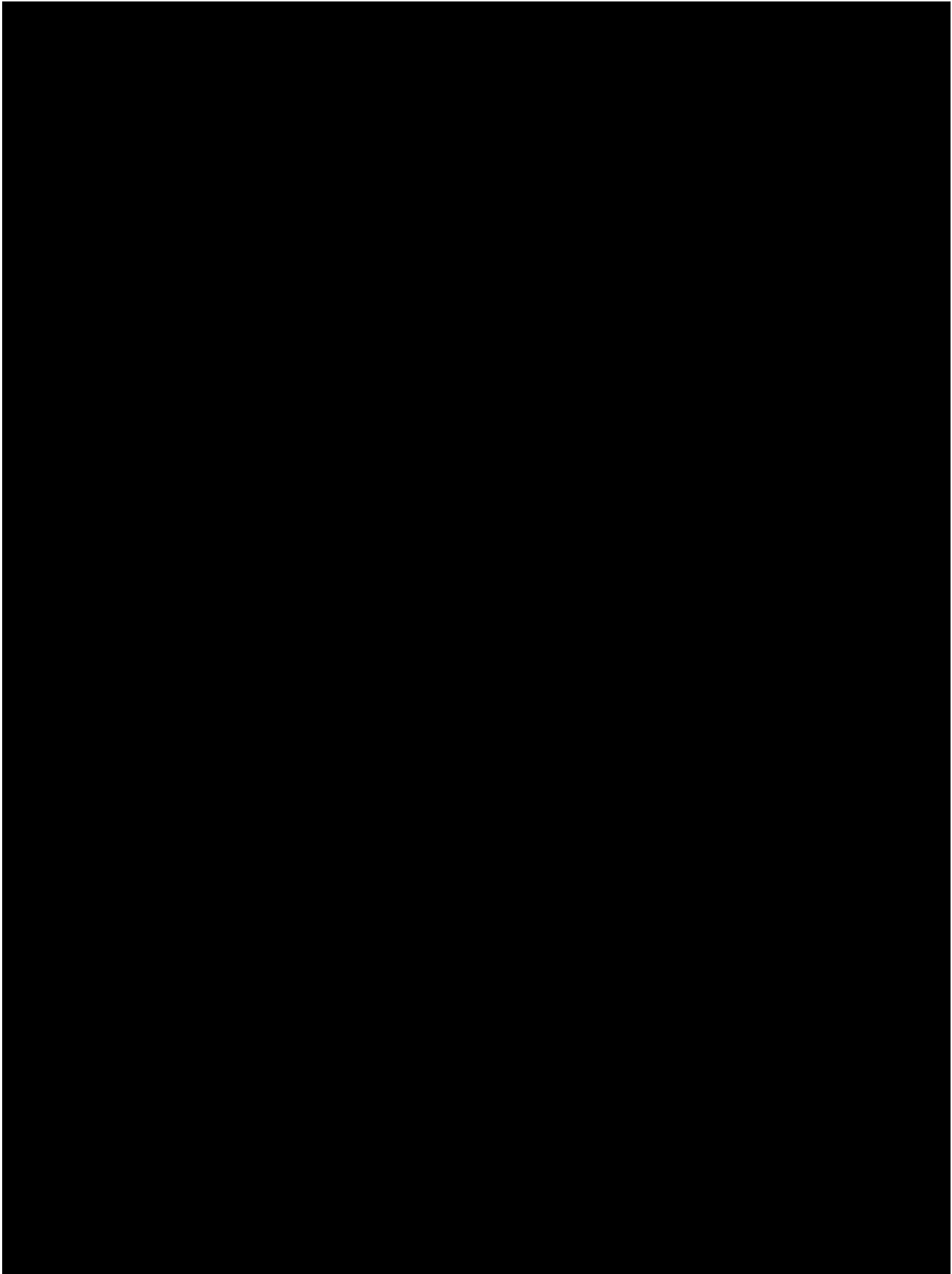


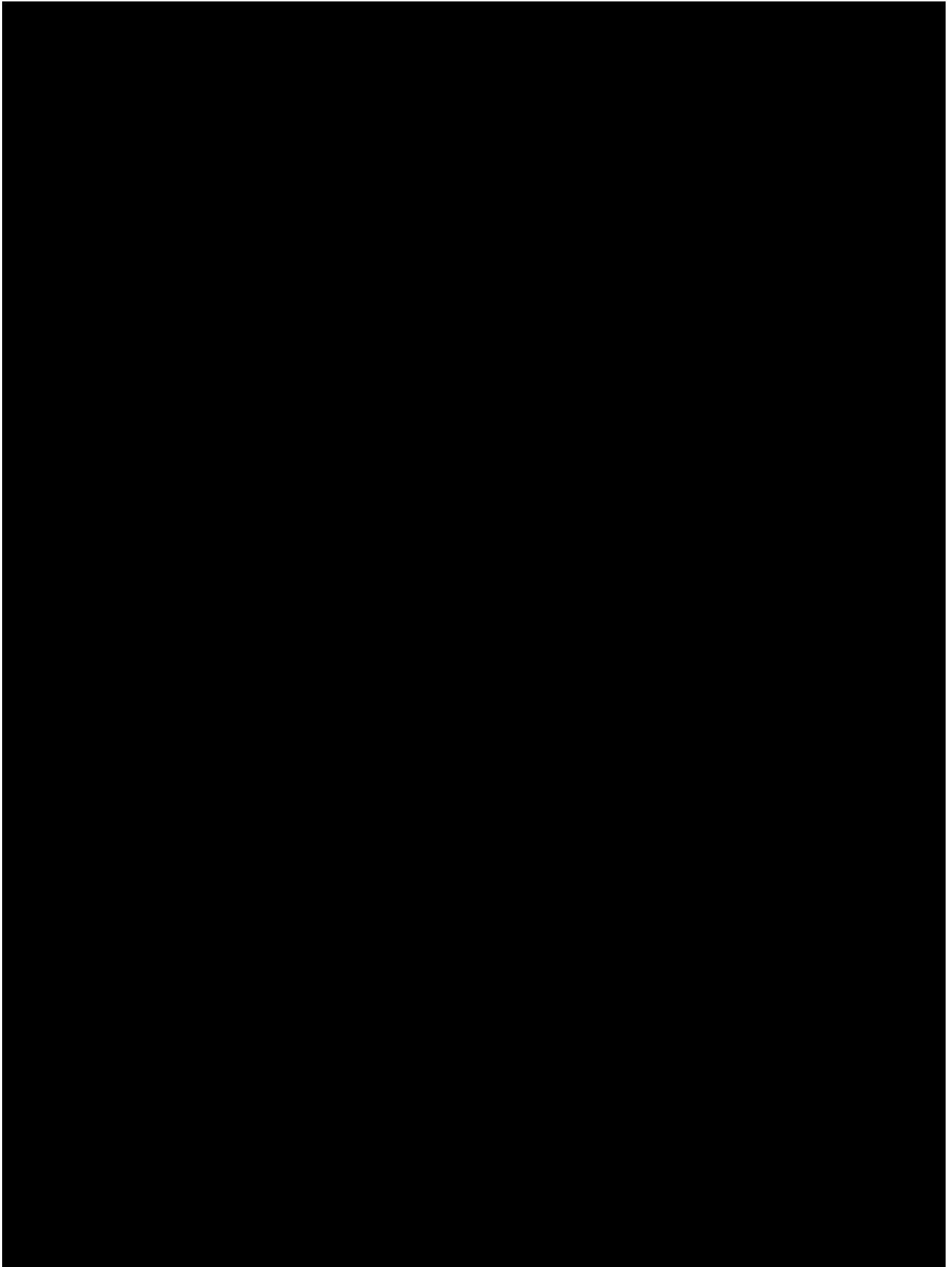


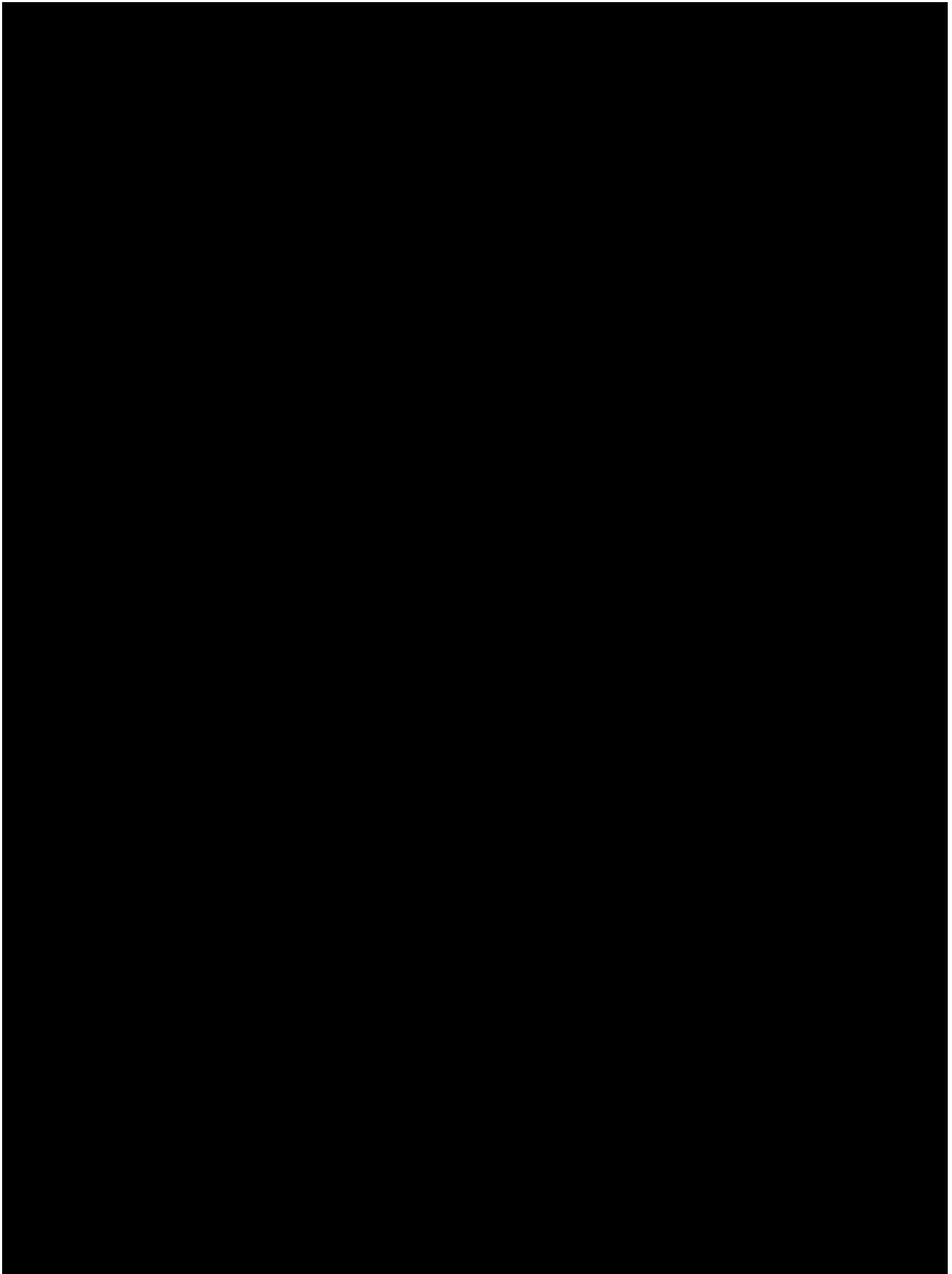


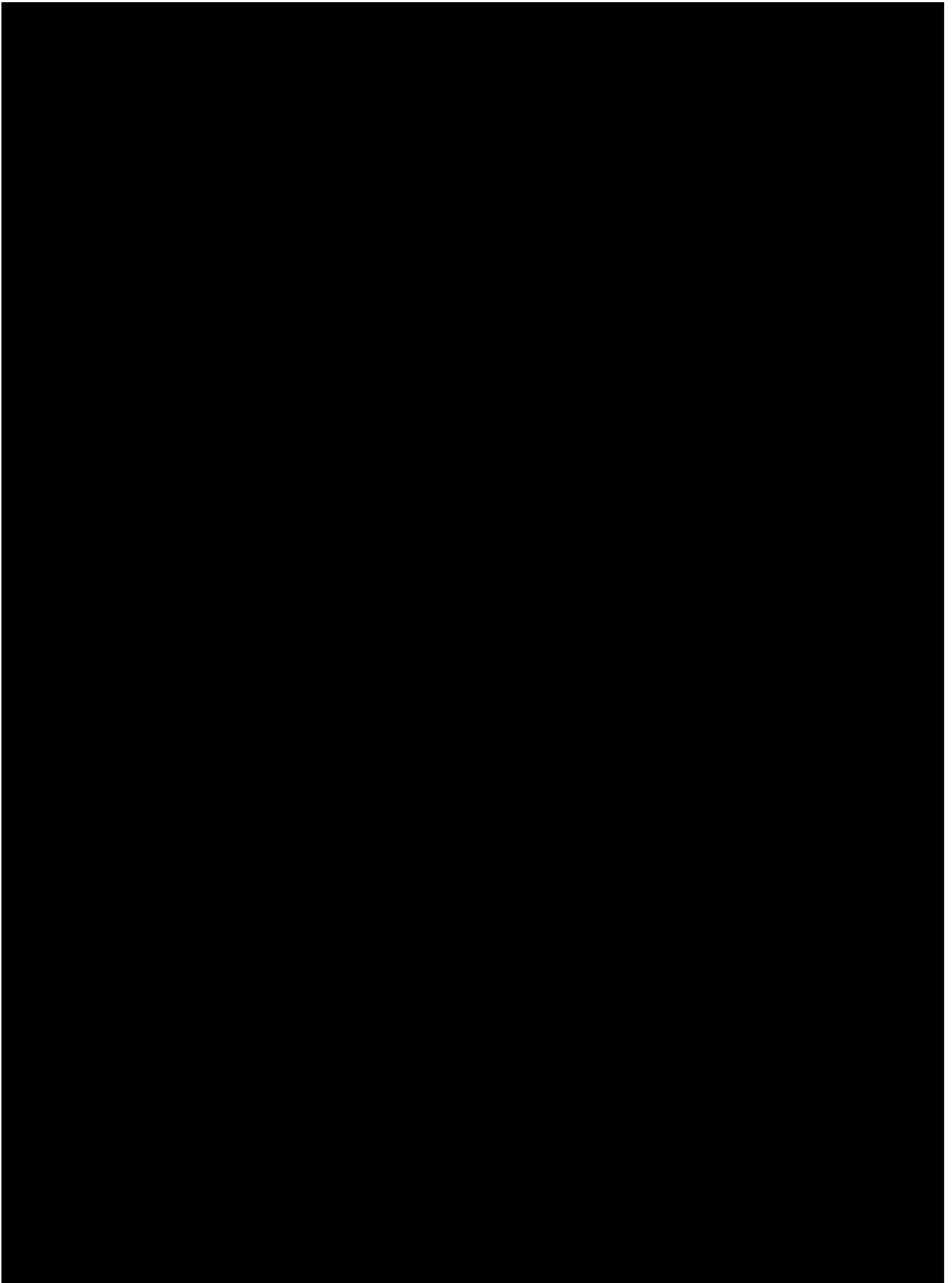


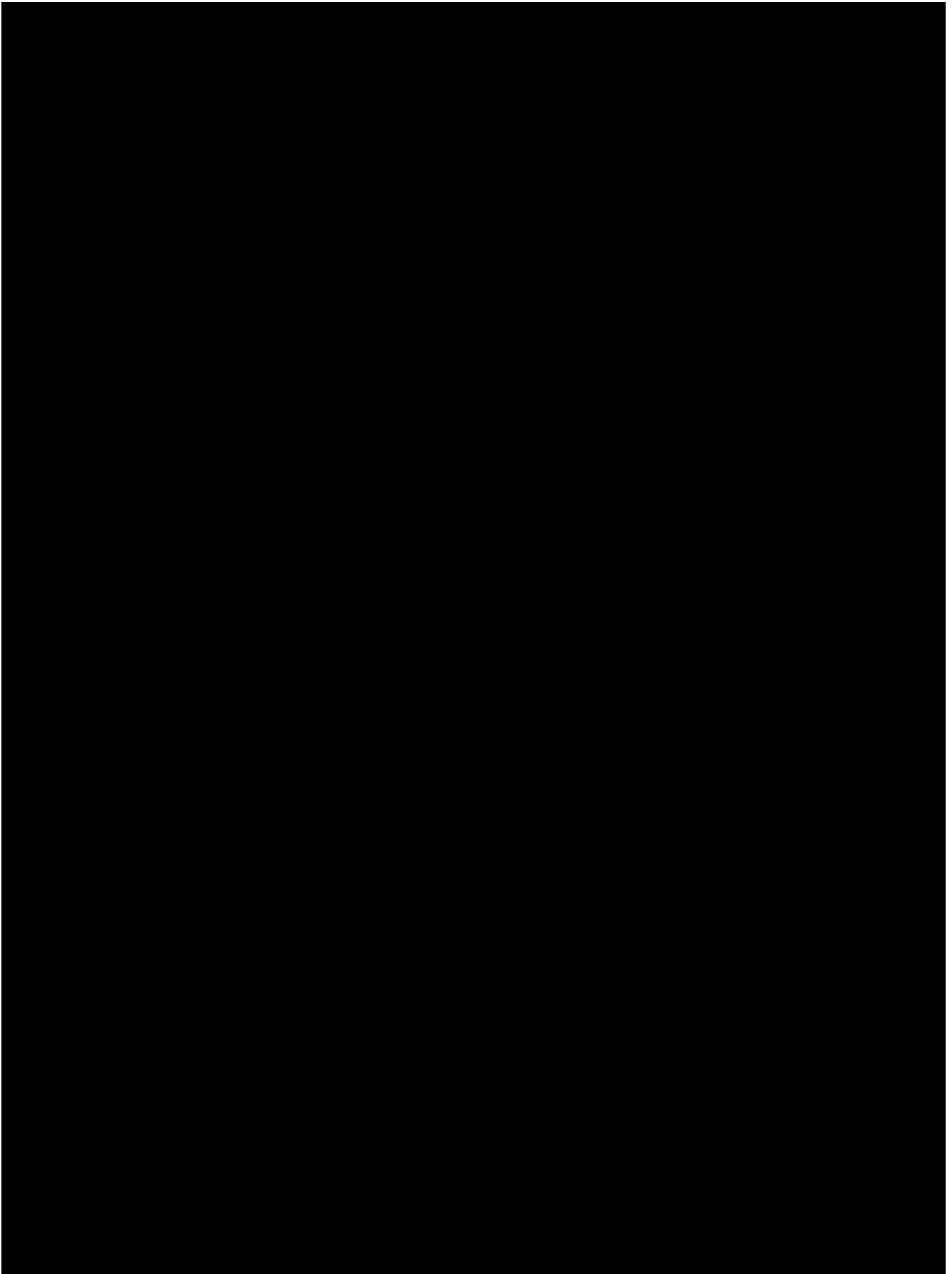


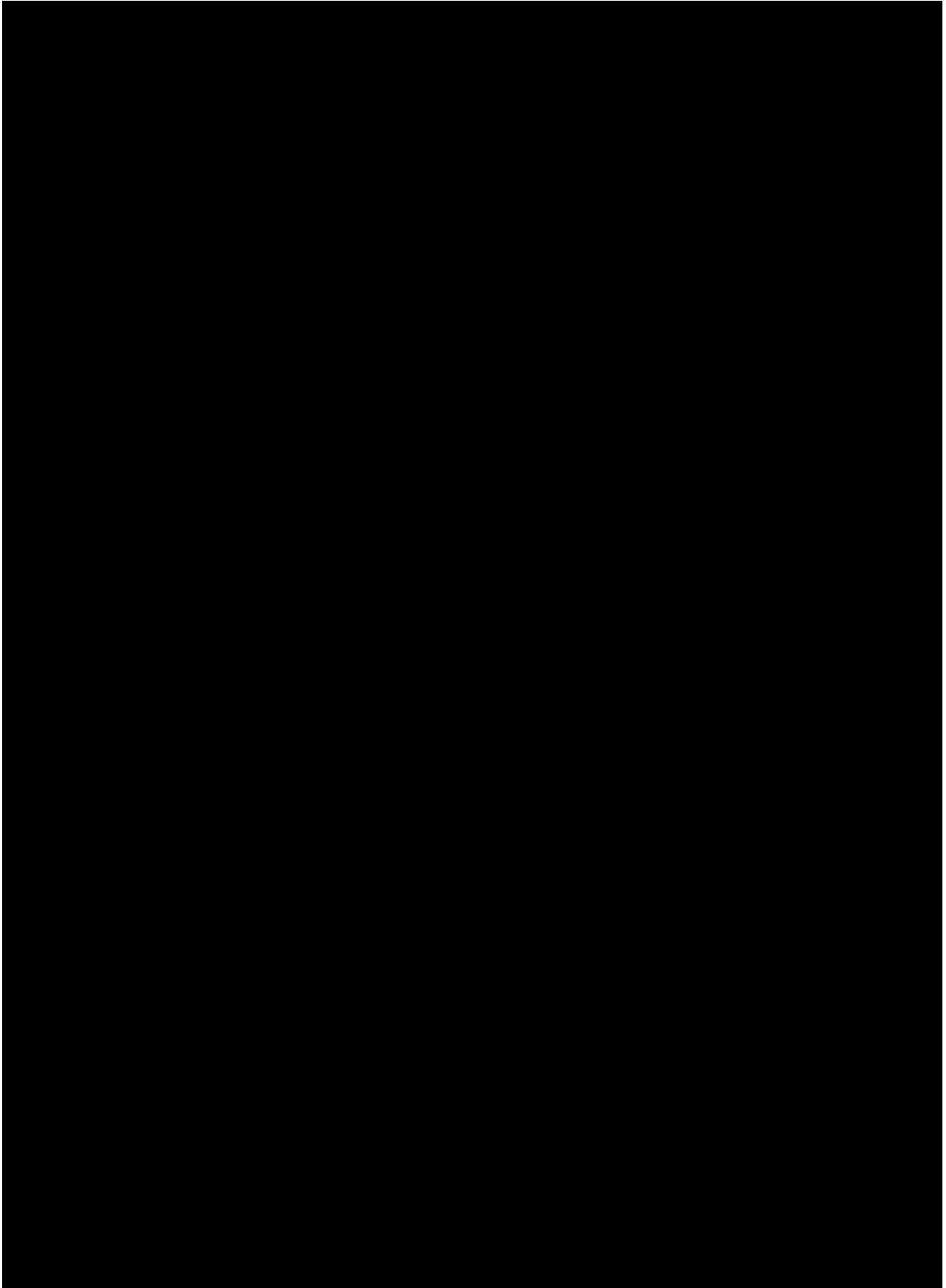


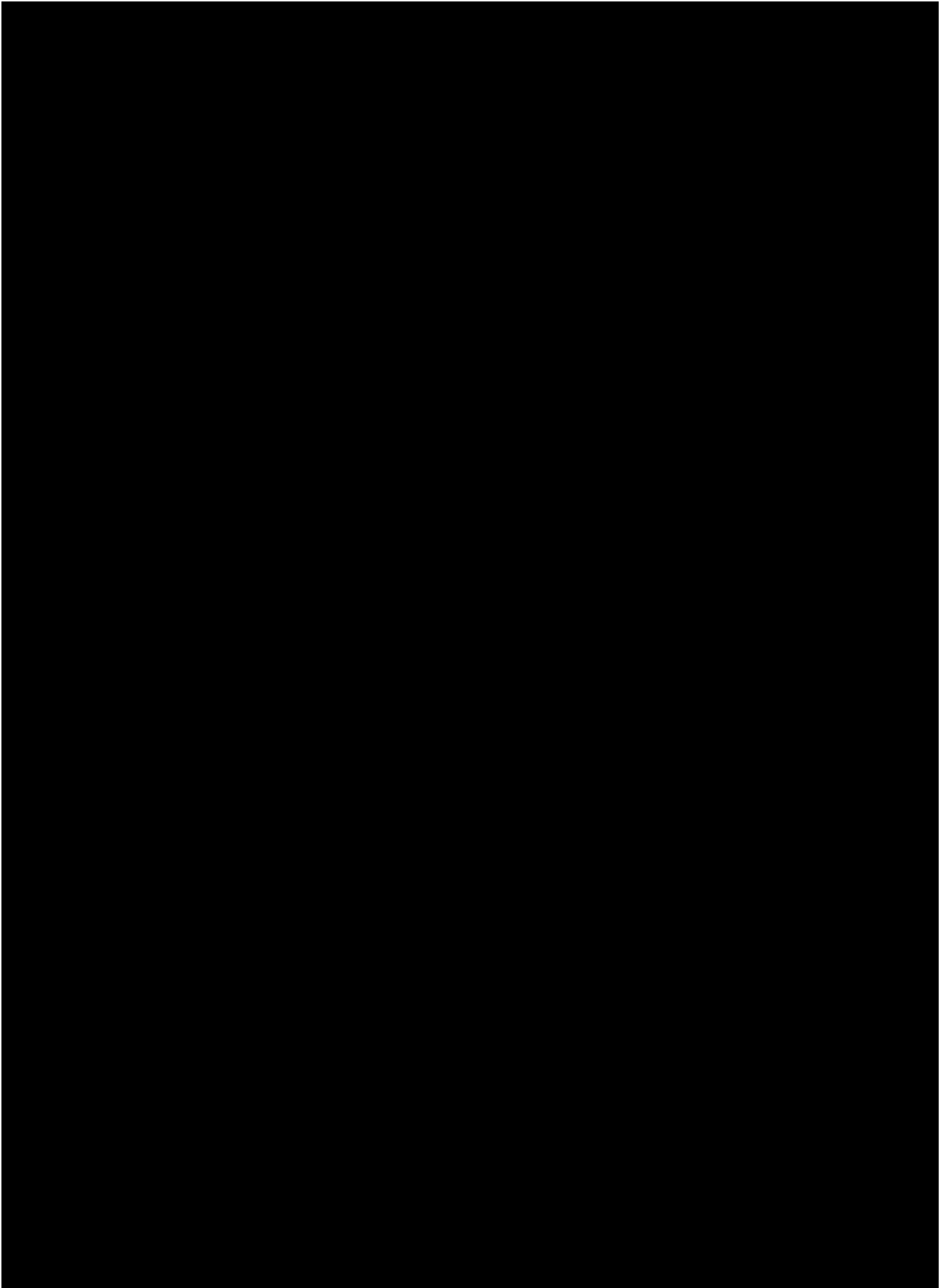


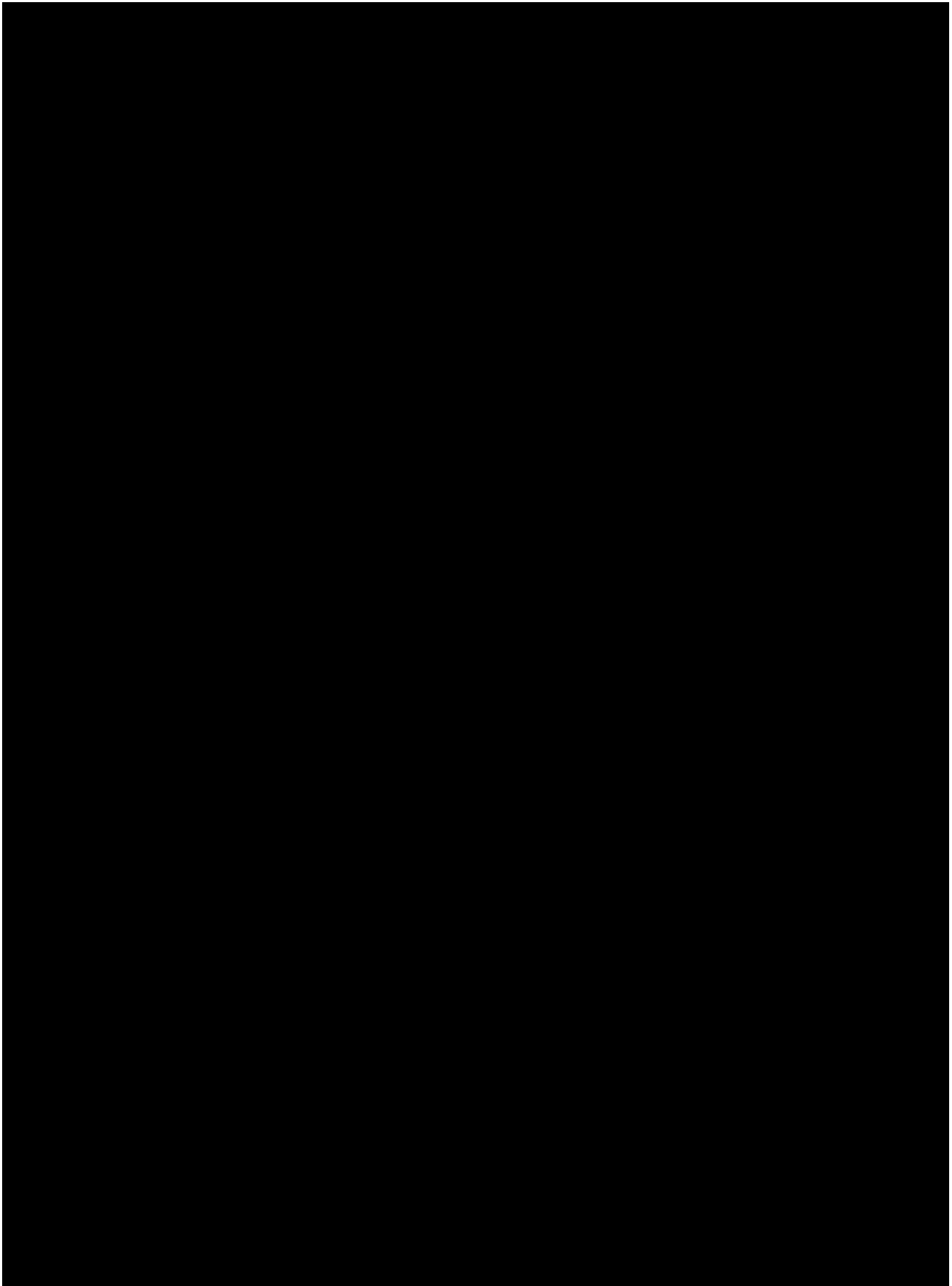


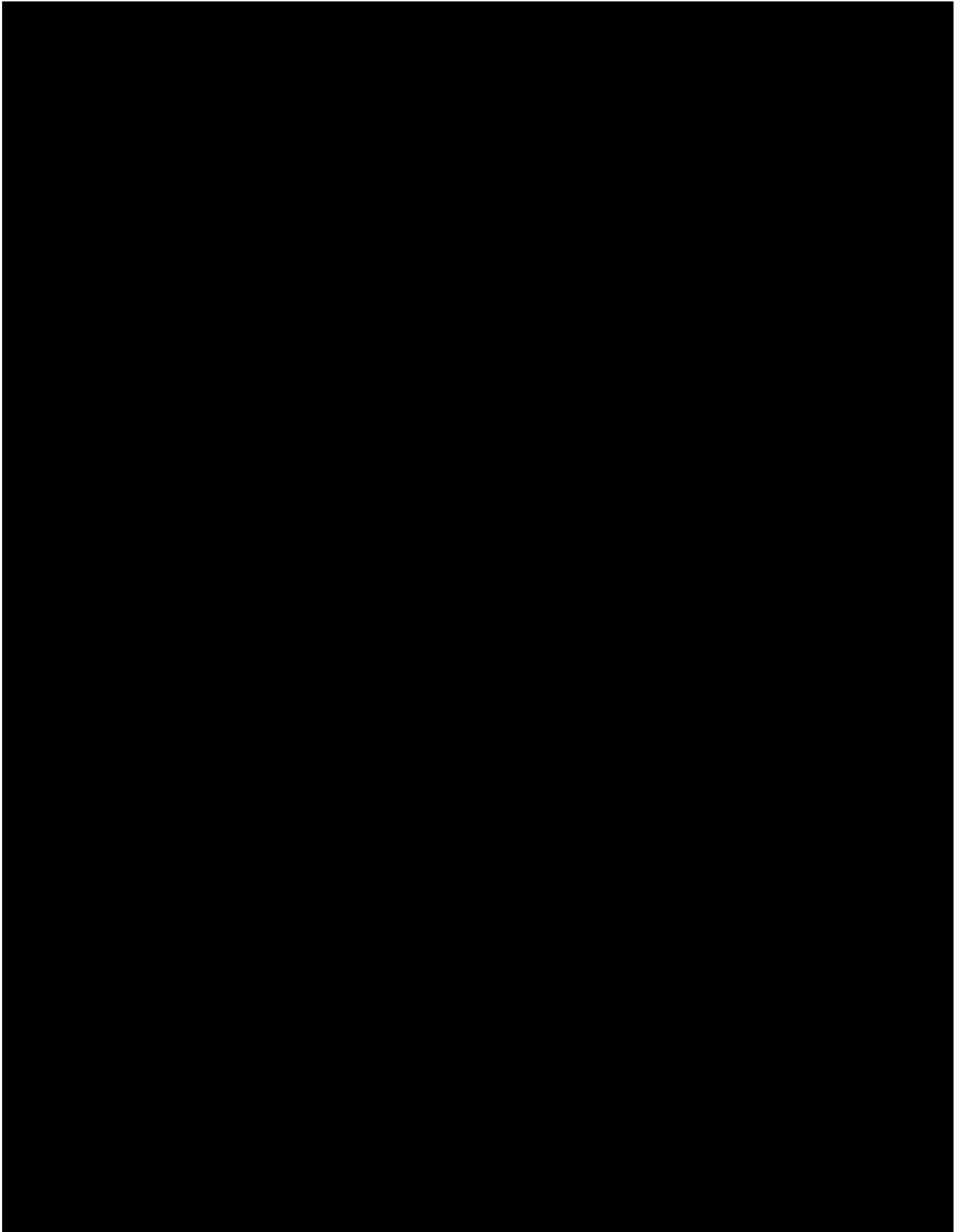


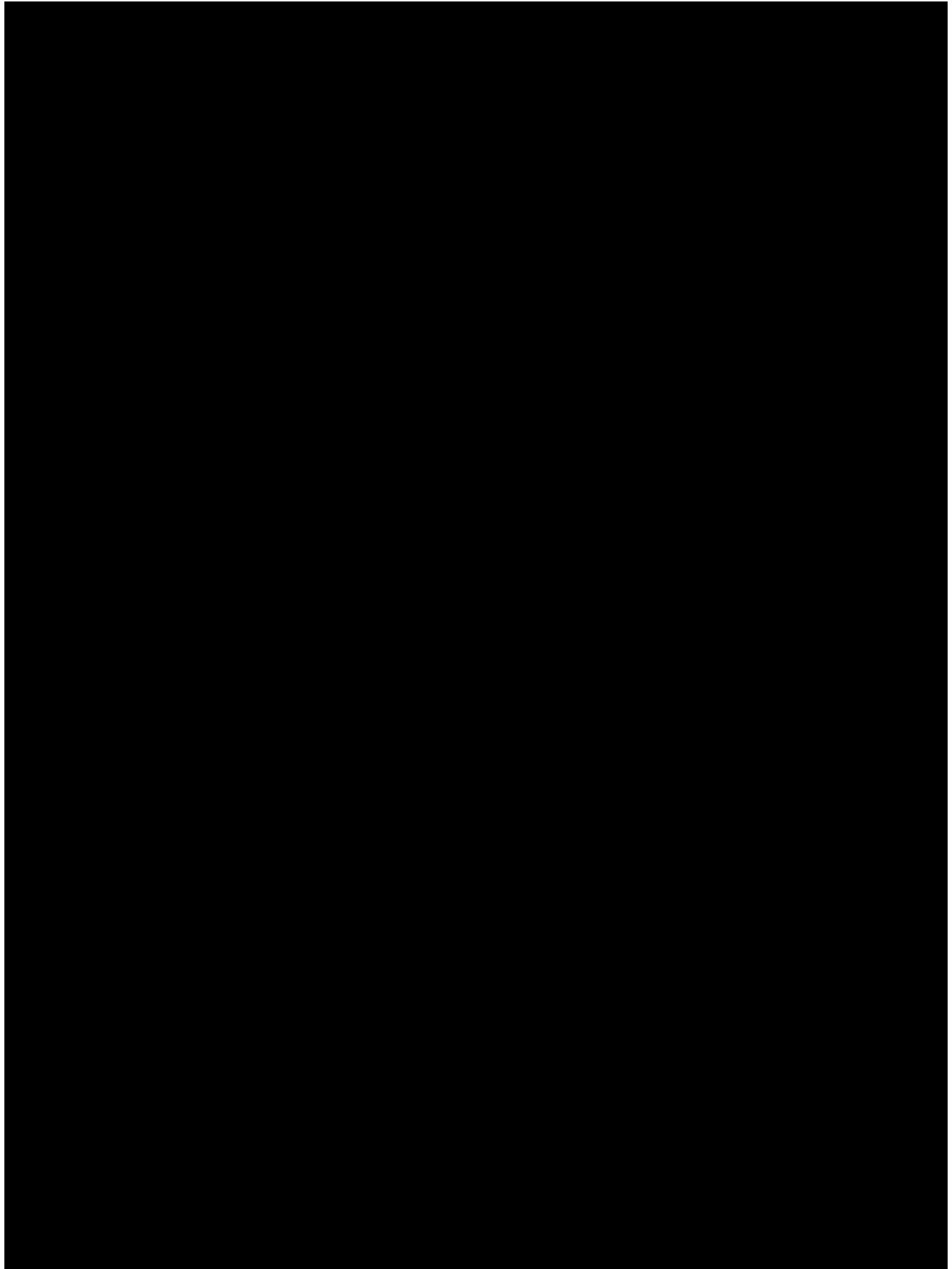


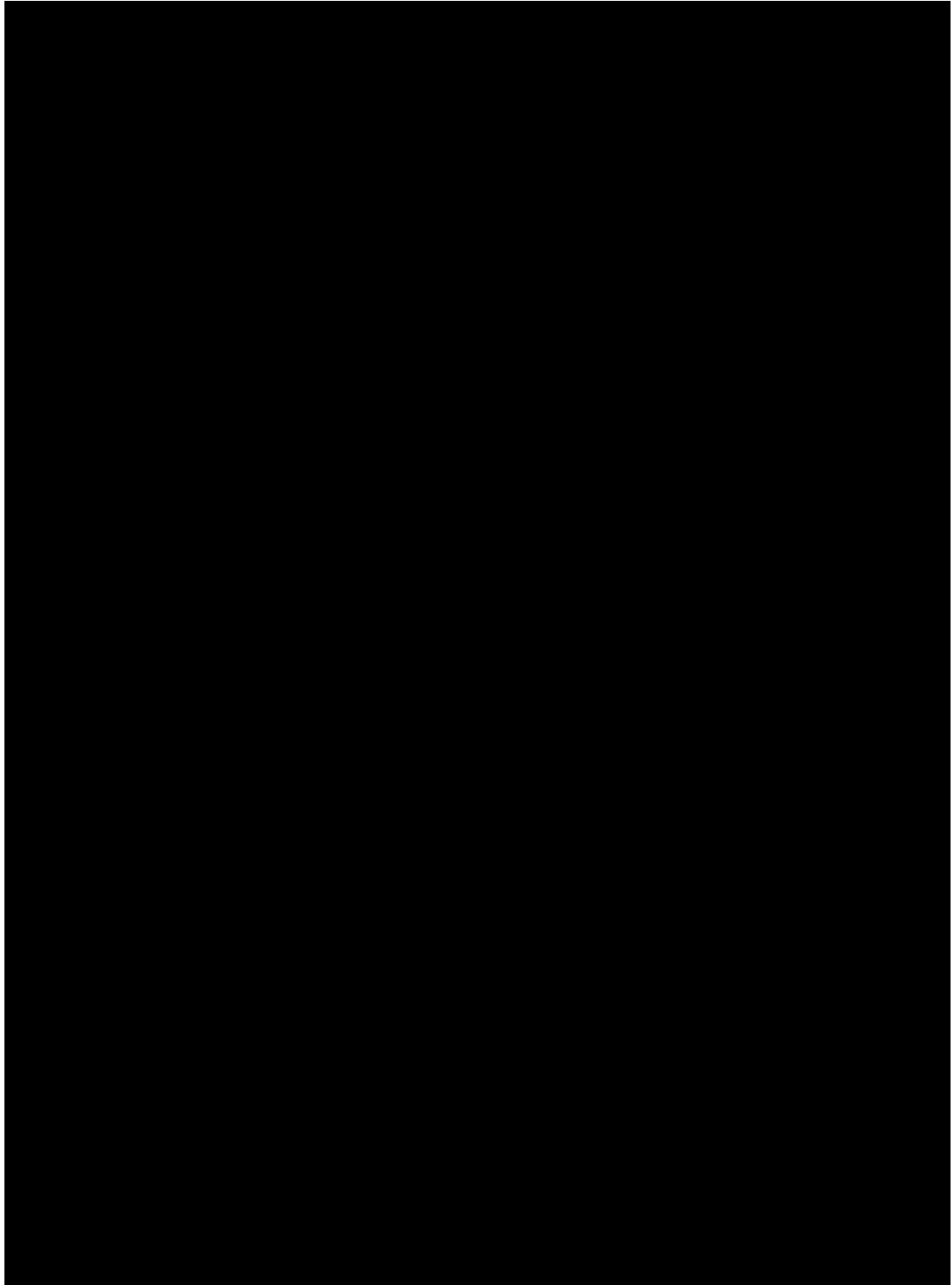


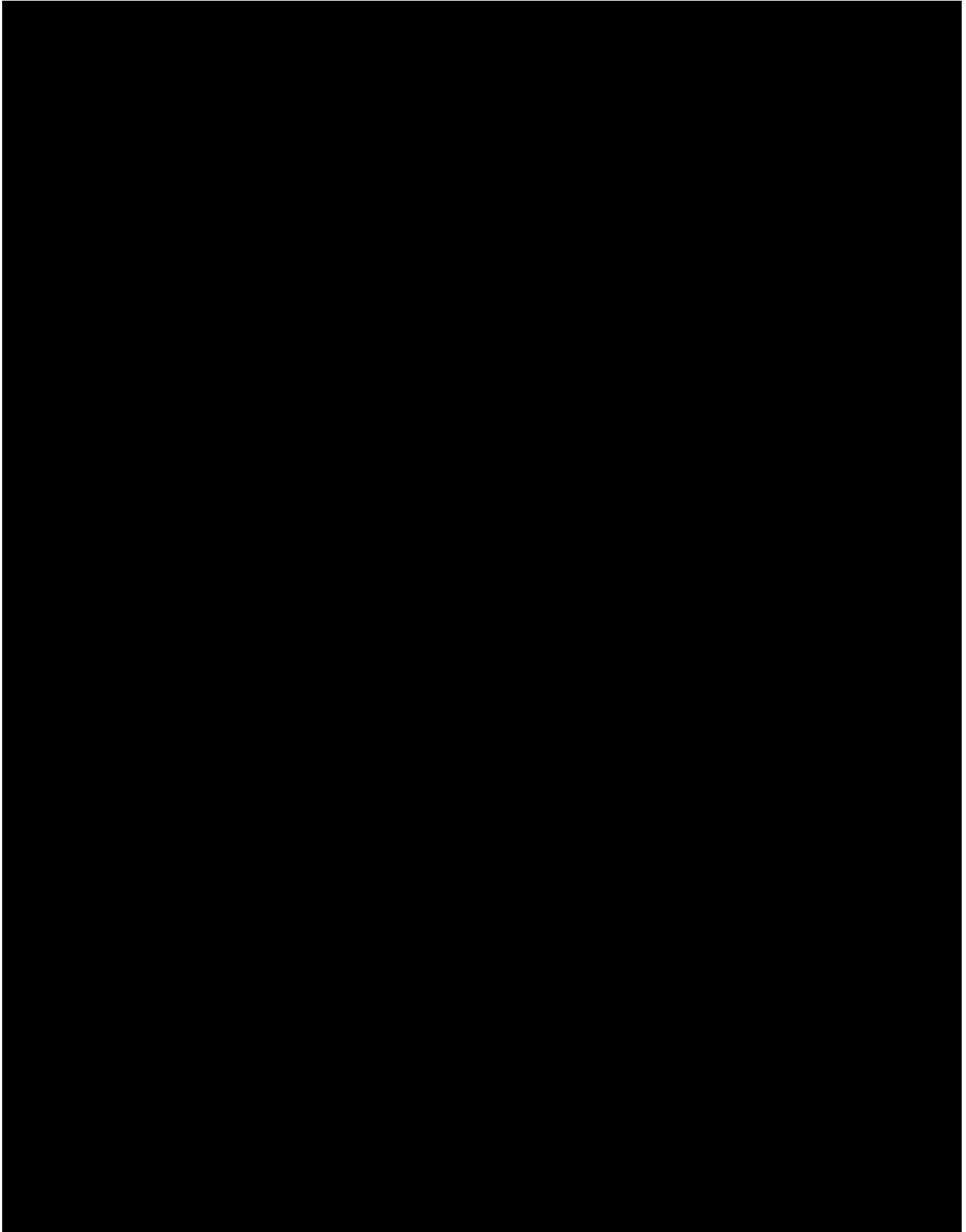


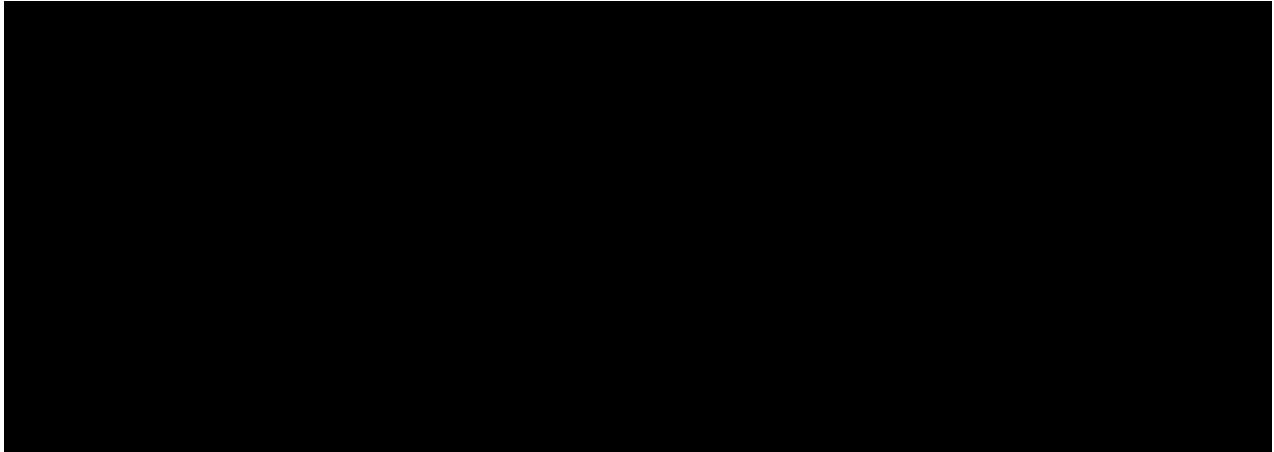




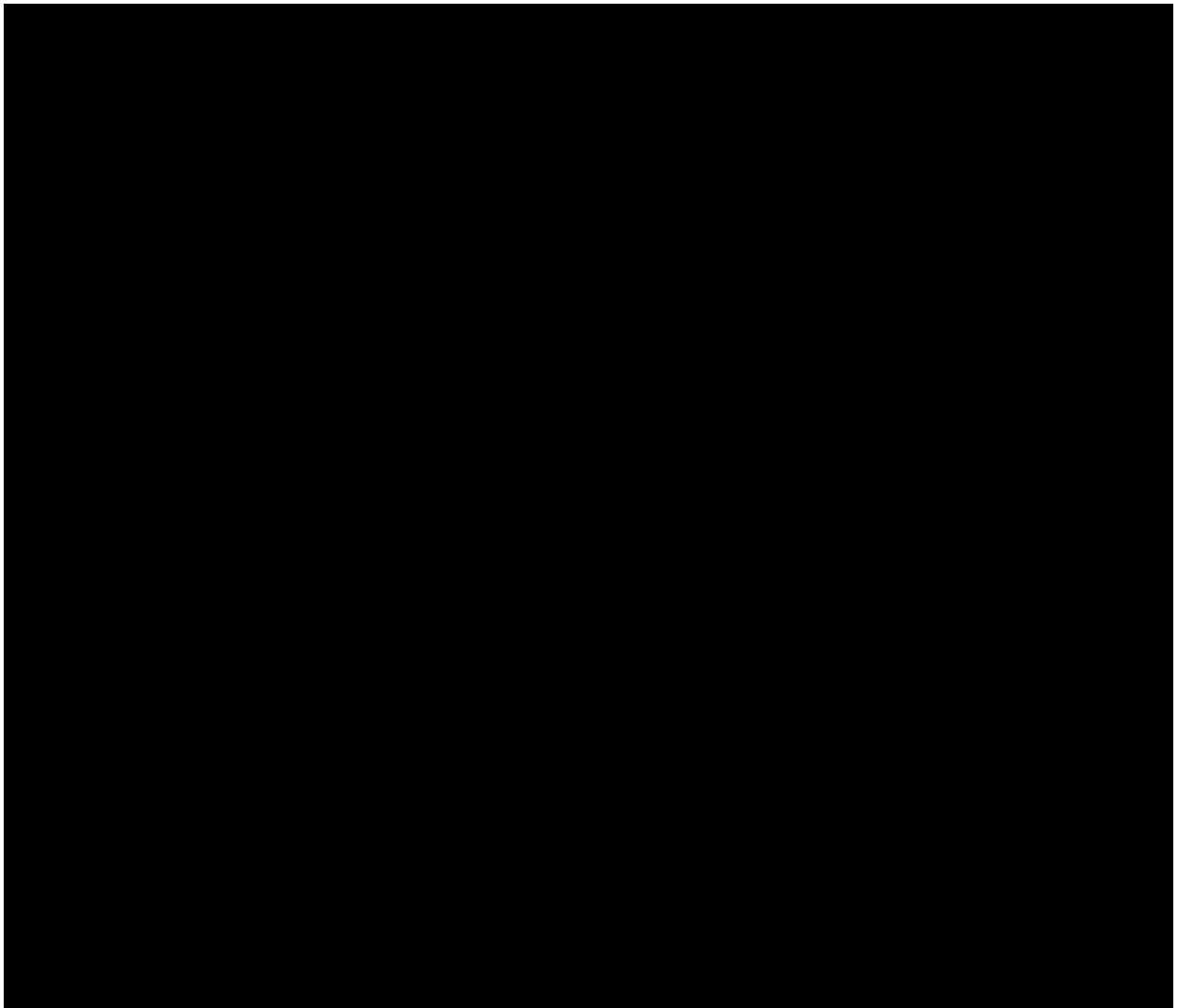


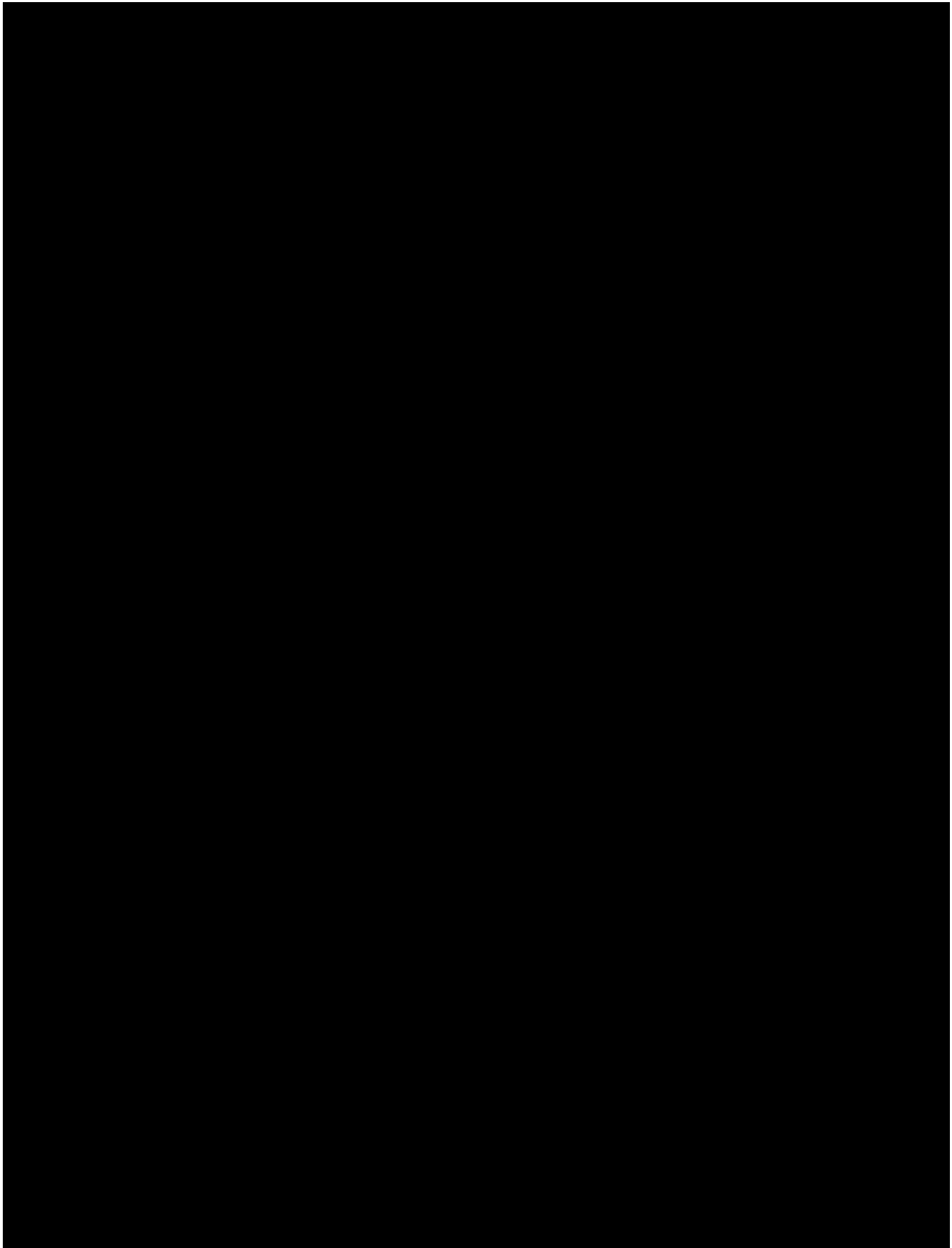


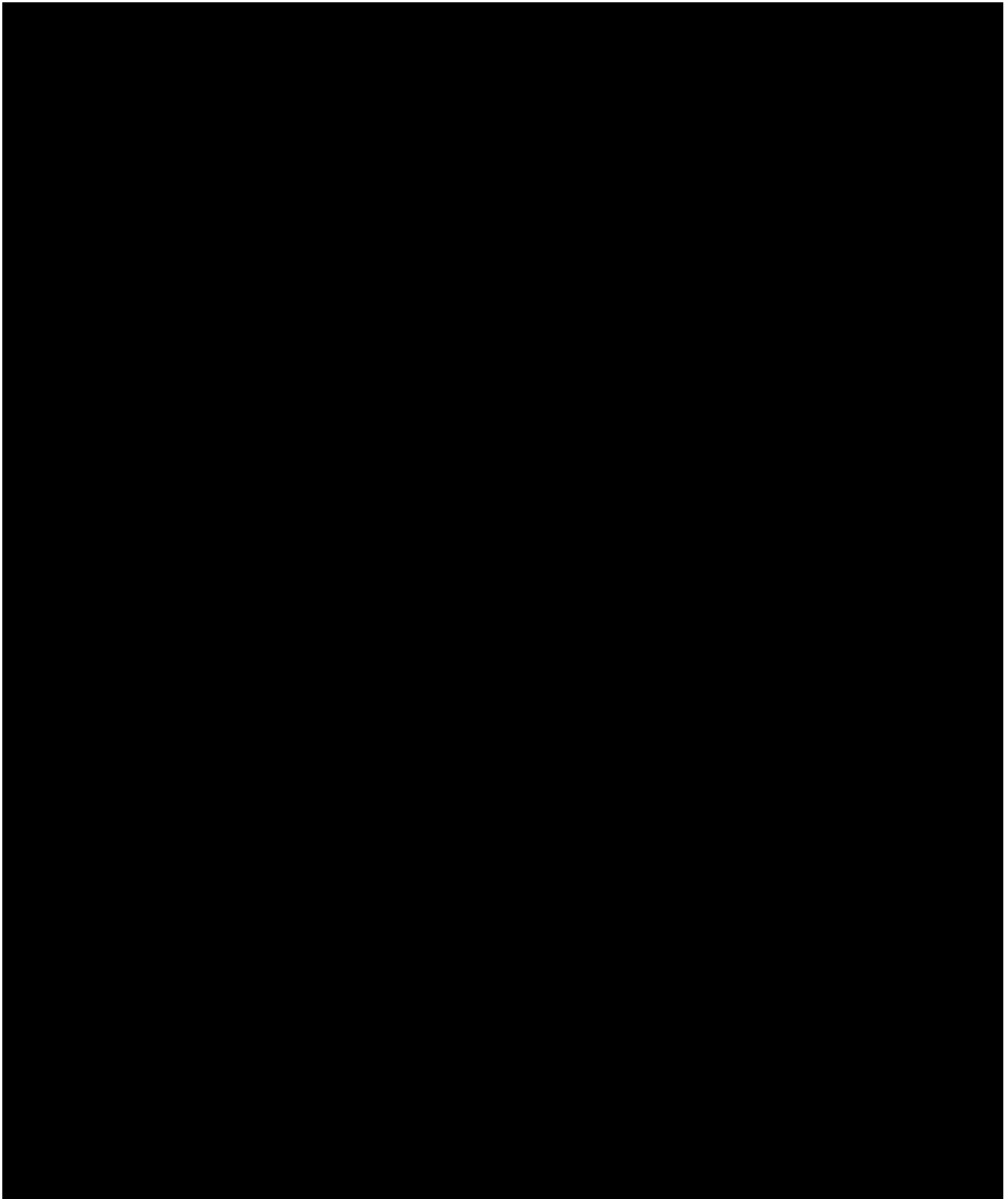




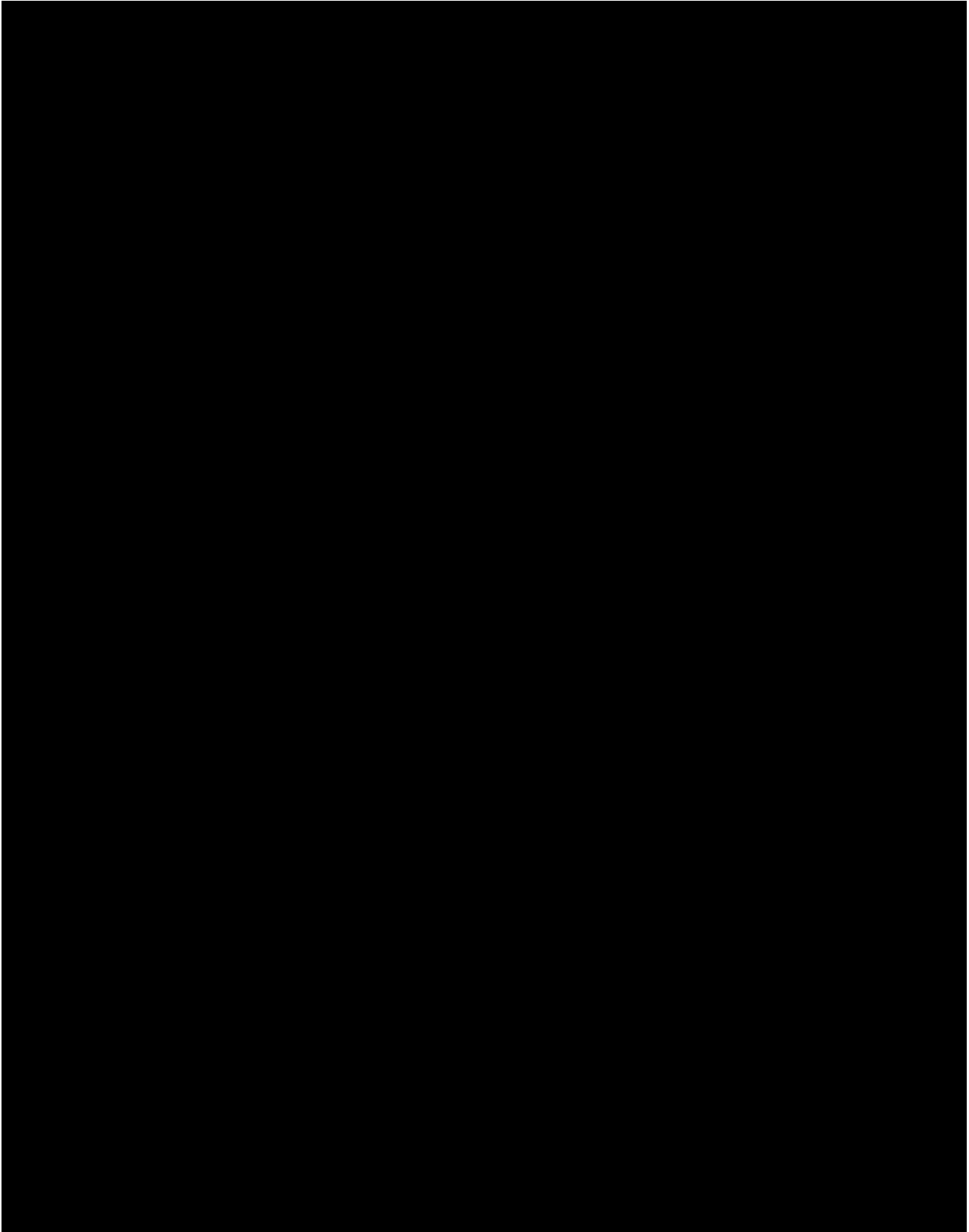
3.4.4 Attachment N, Subsidy Provider Compliance Business Specifications

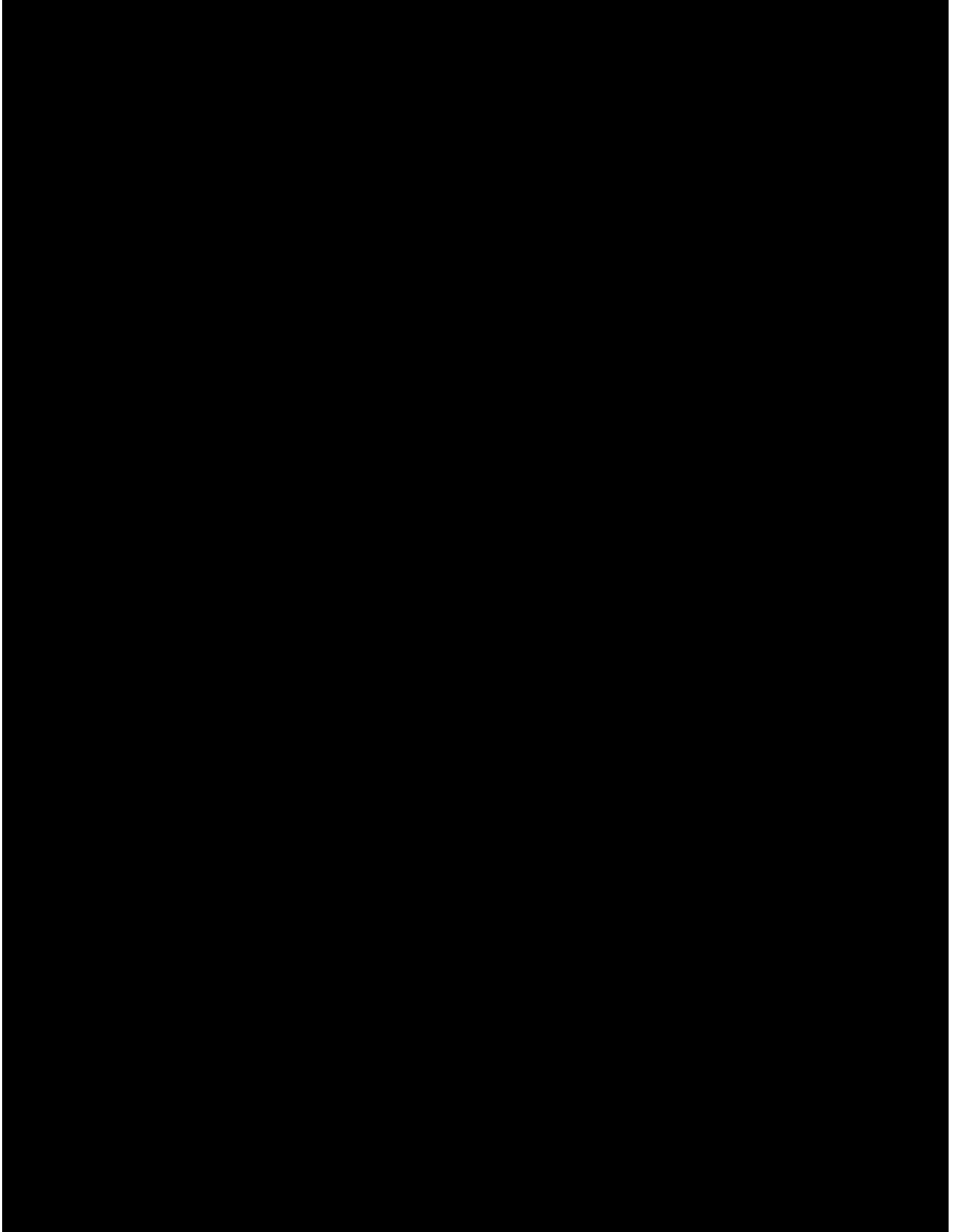


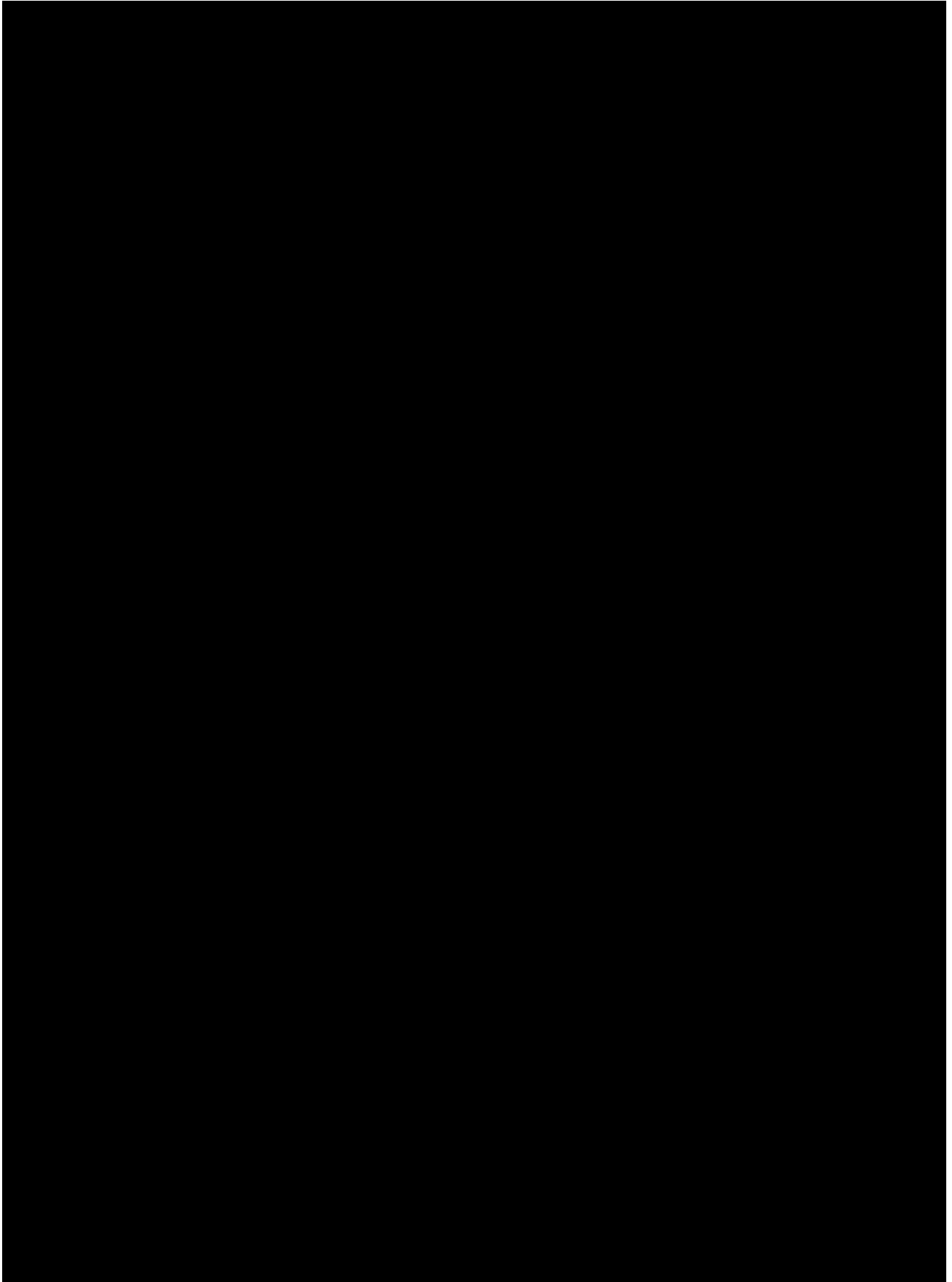


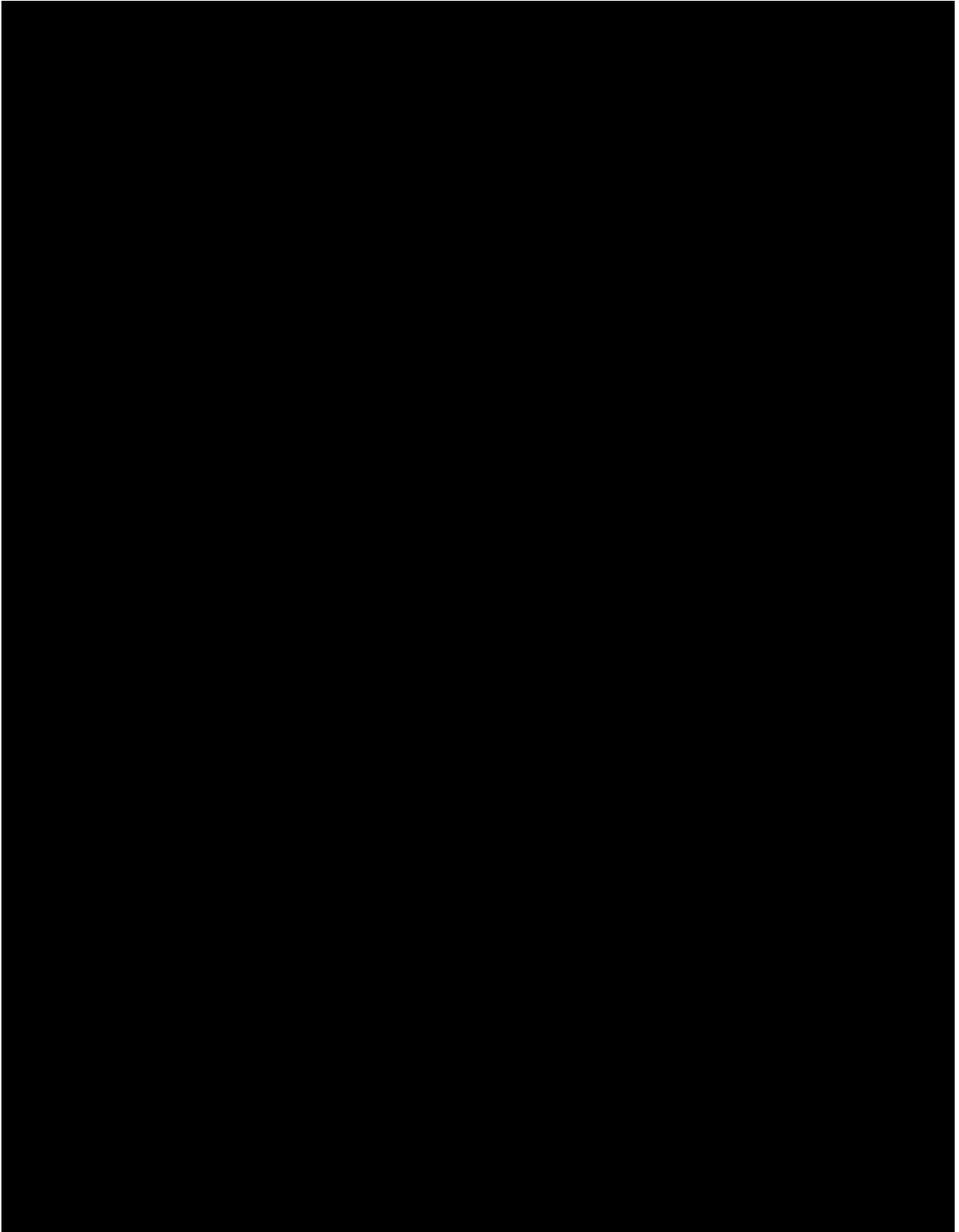


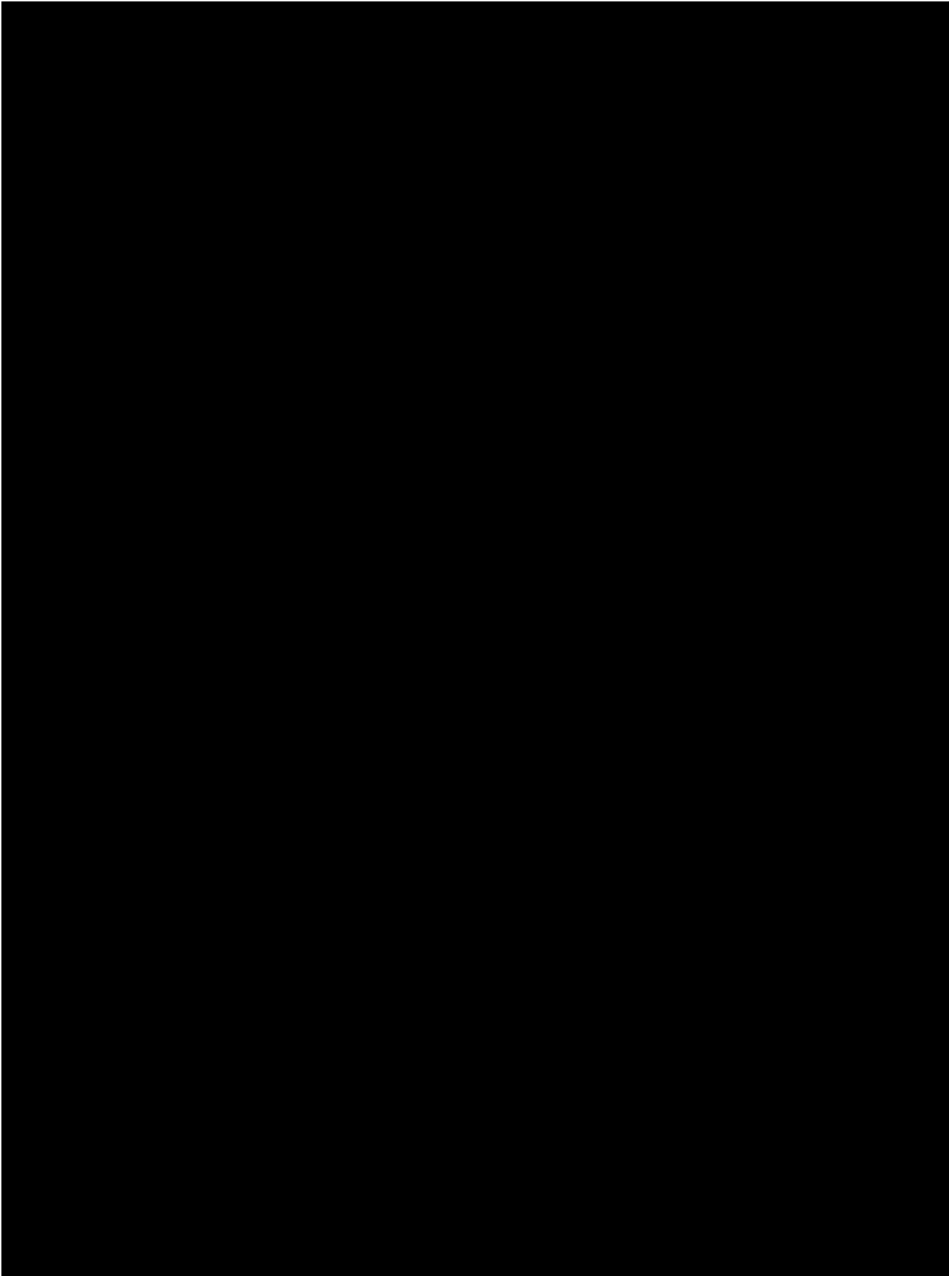
3.4.5 Attachment O, Business and Technical Specifications

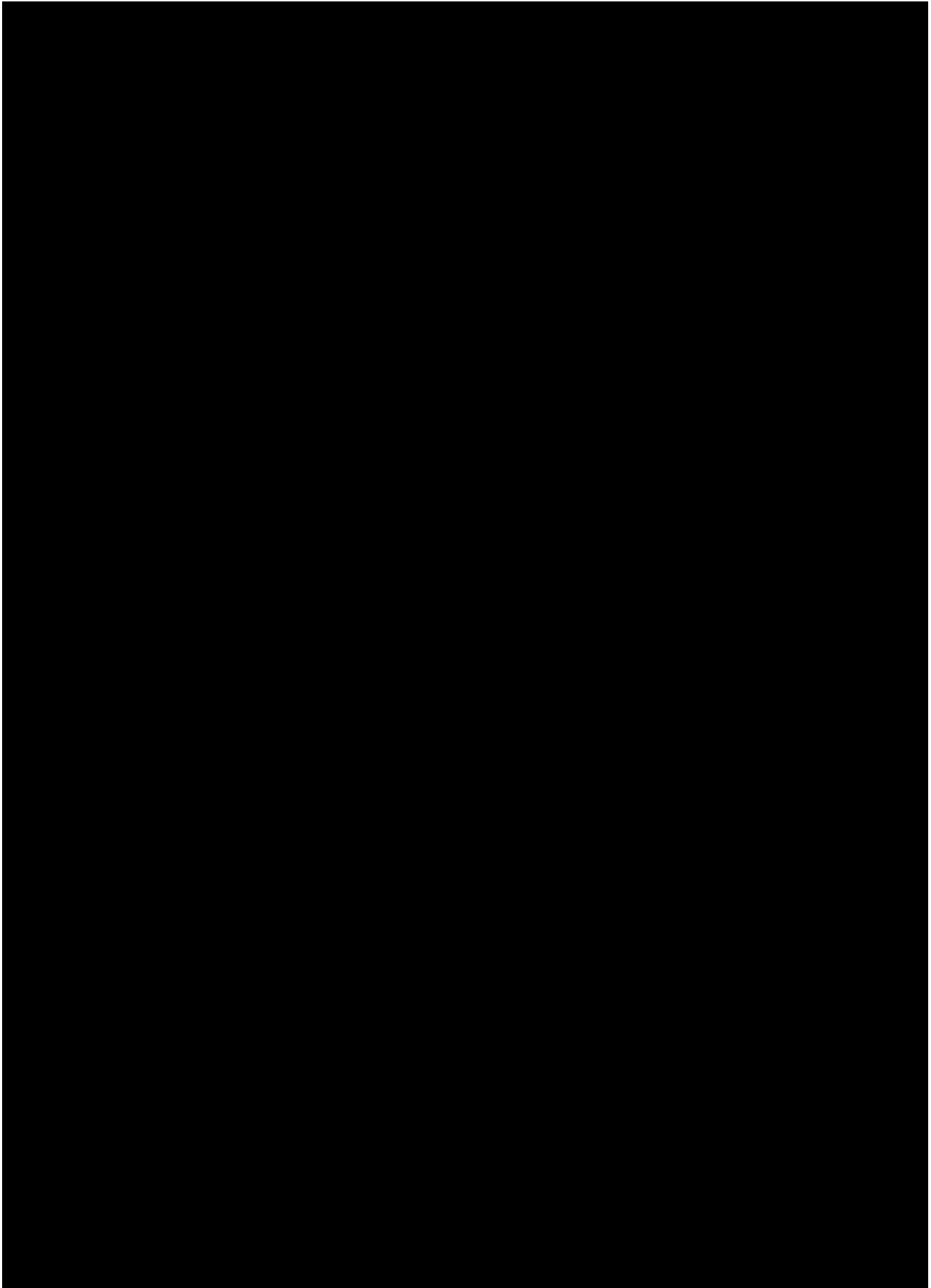


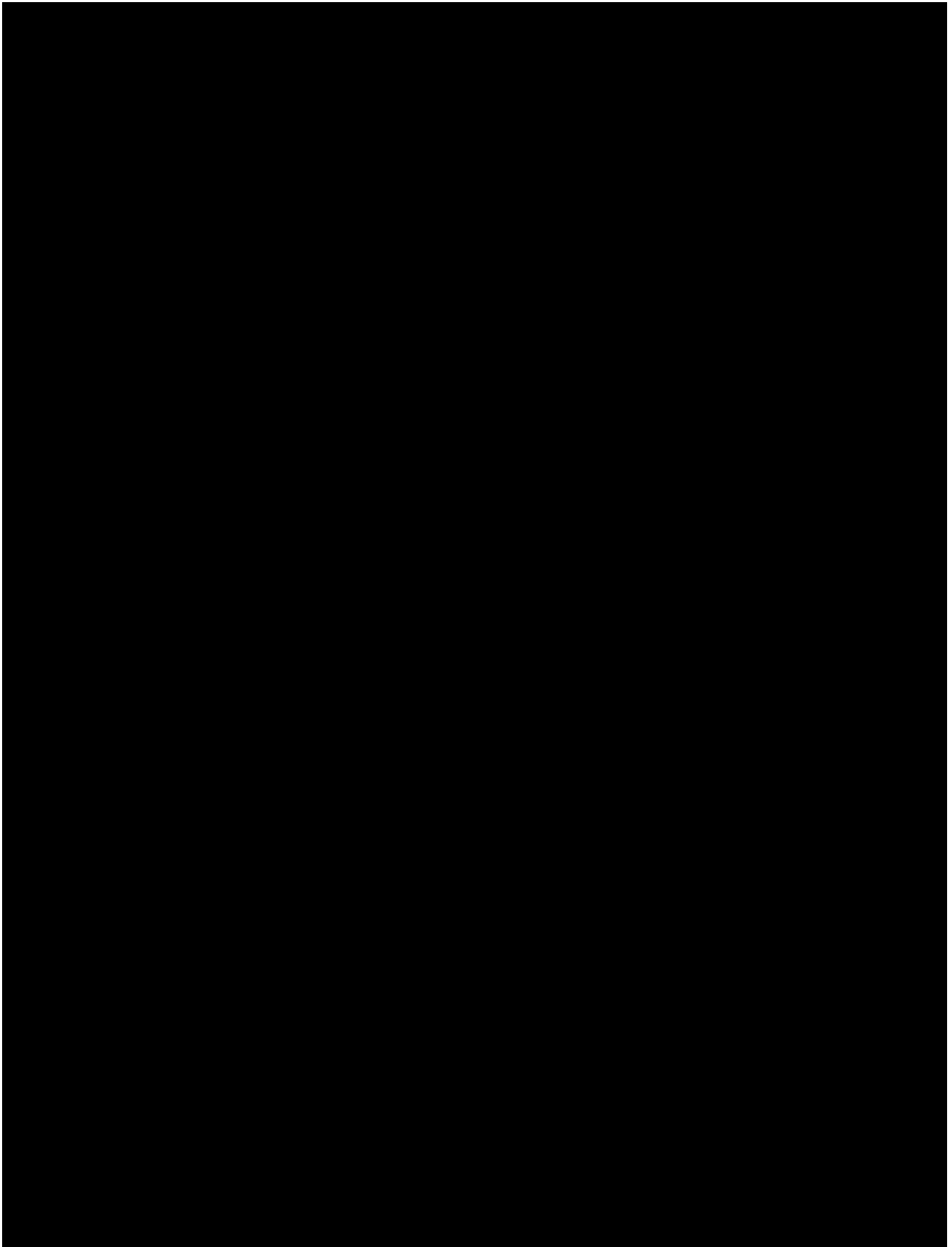


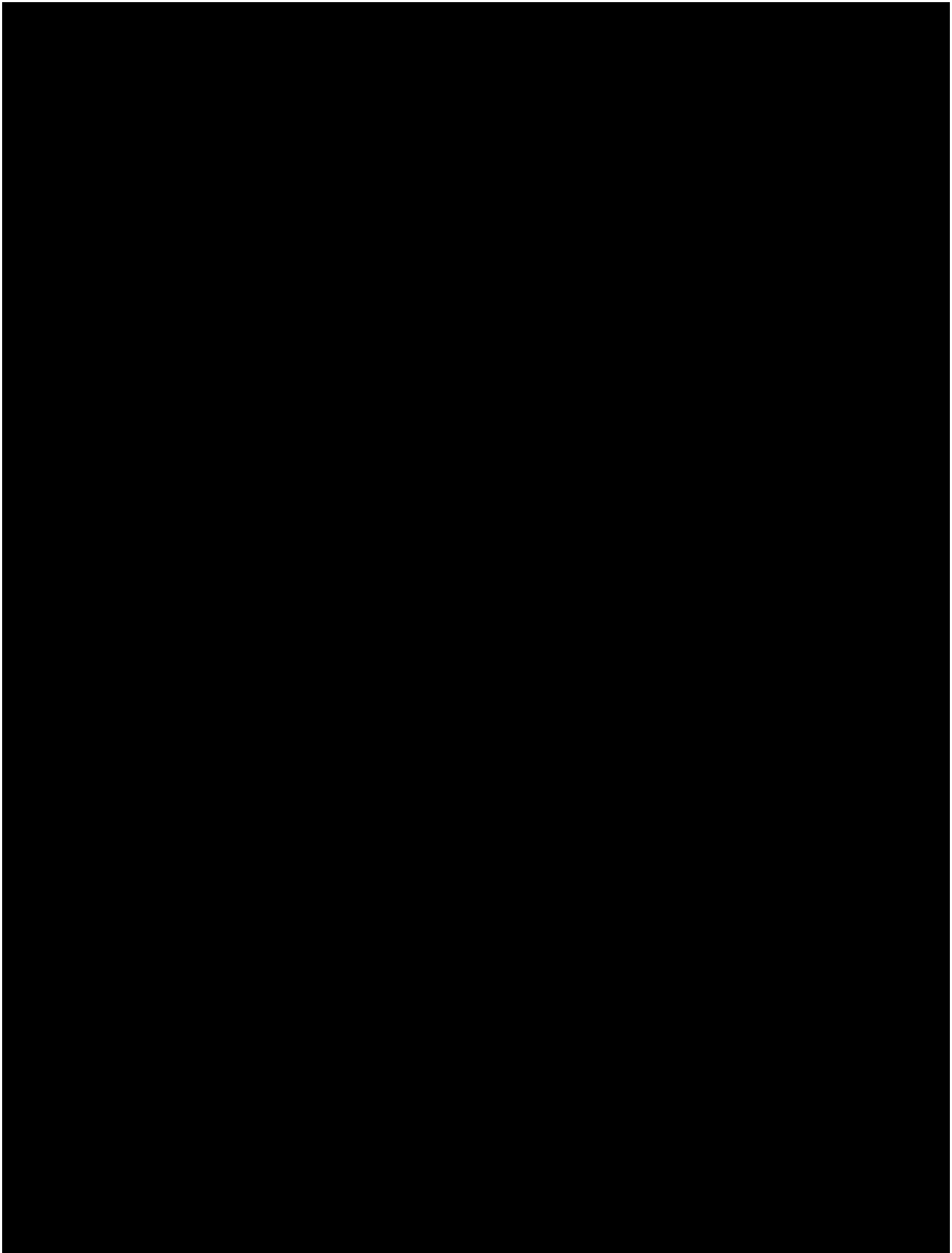


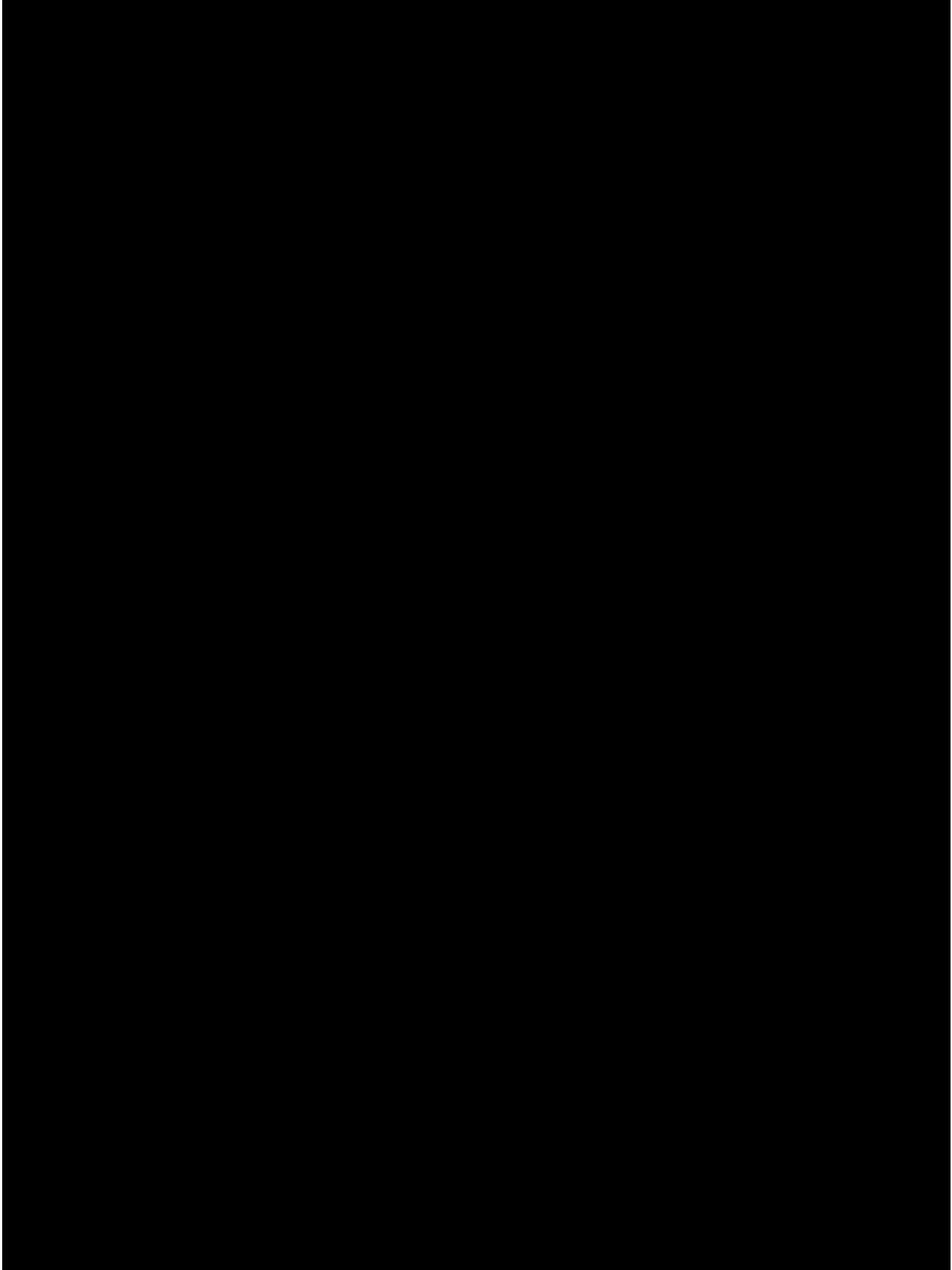


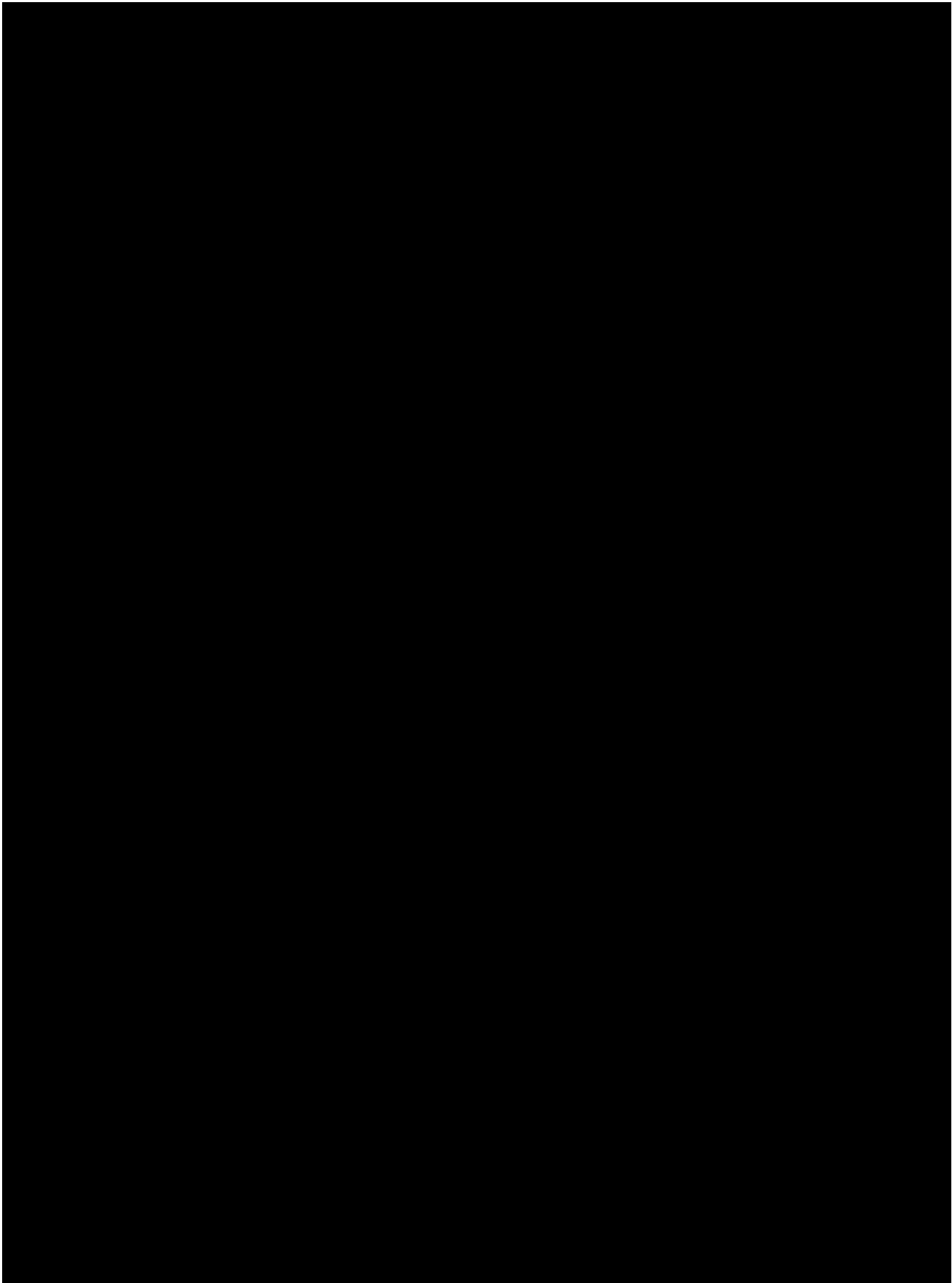


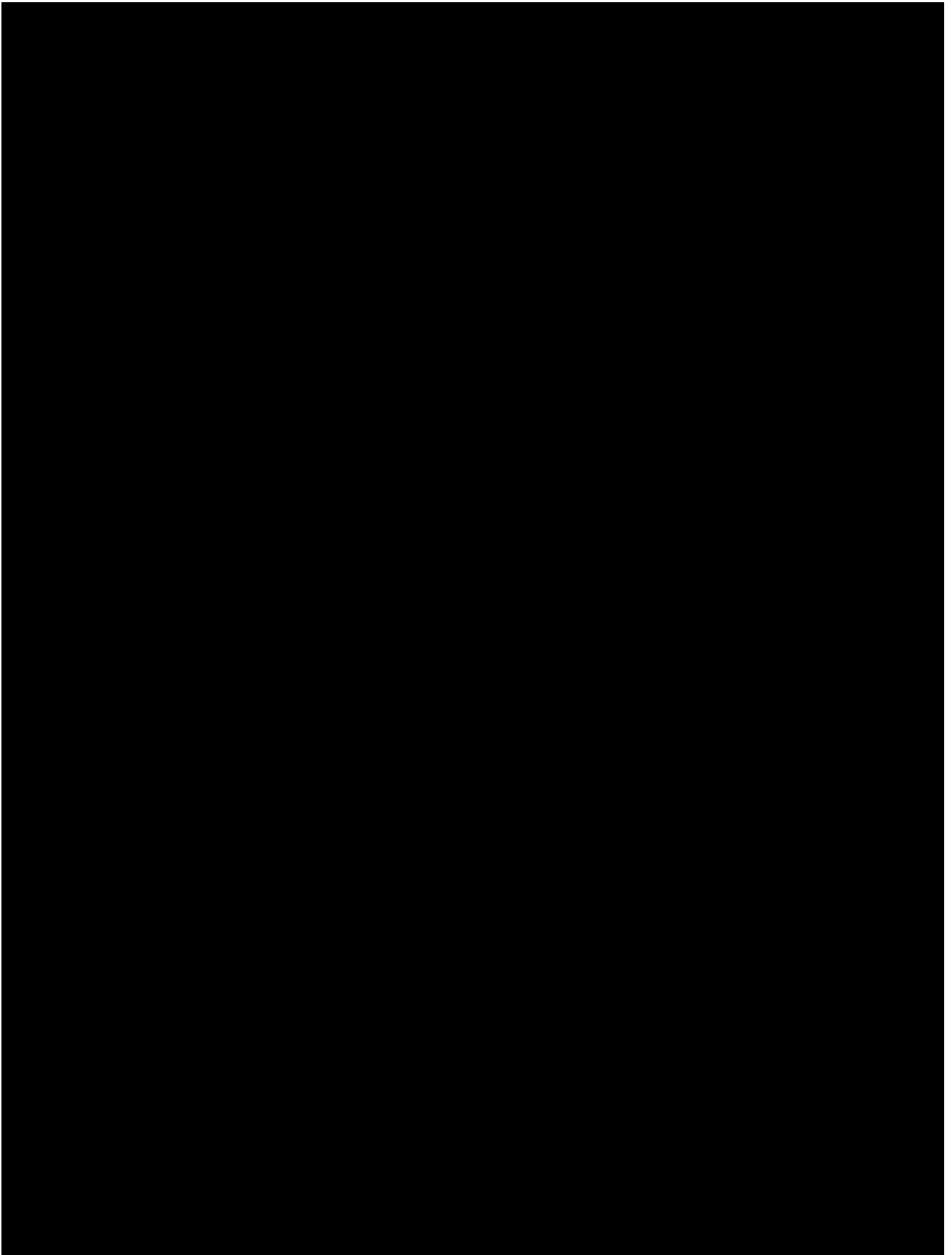


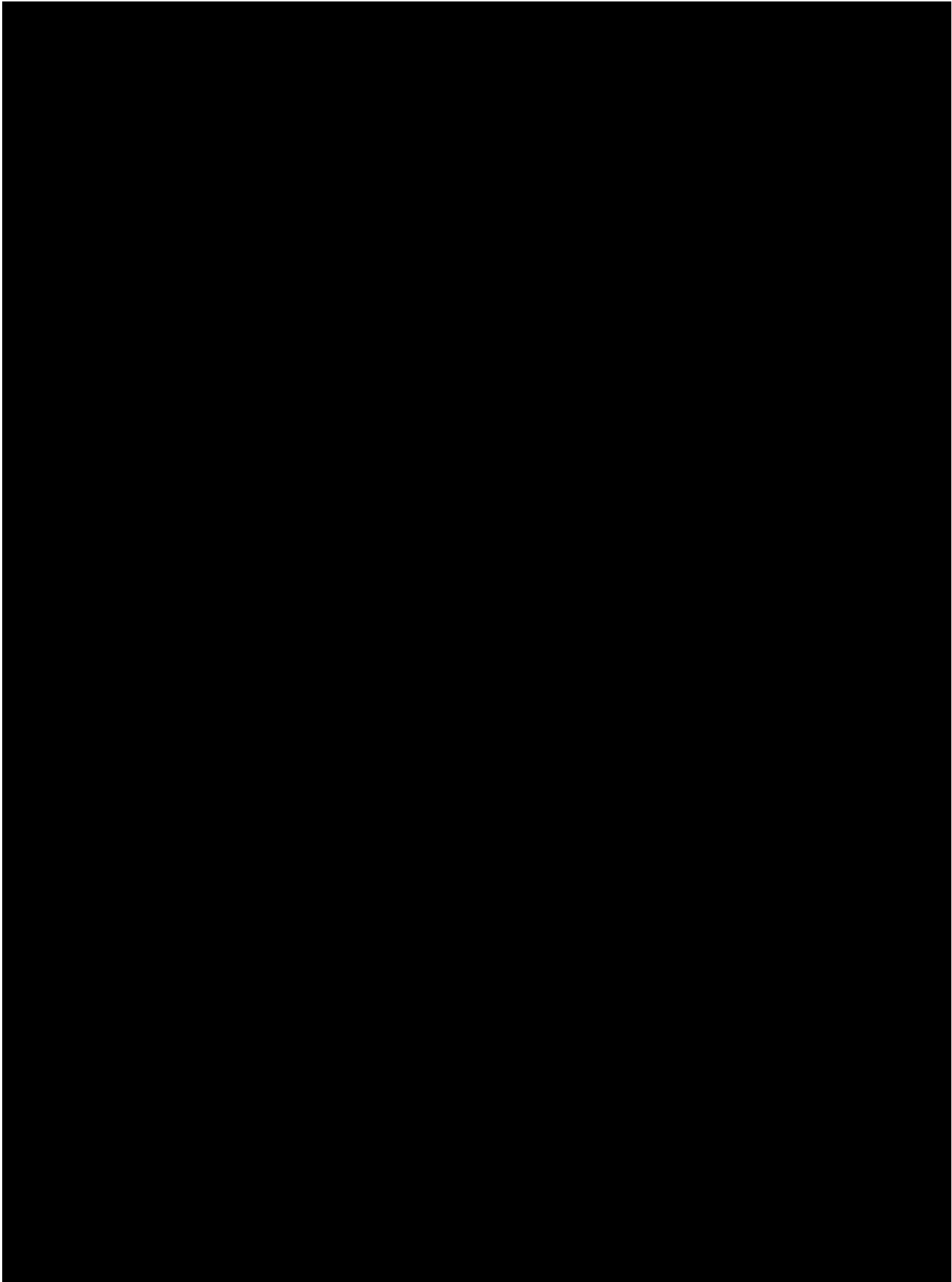


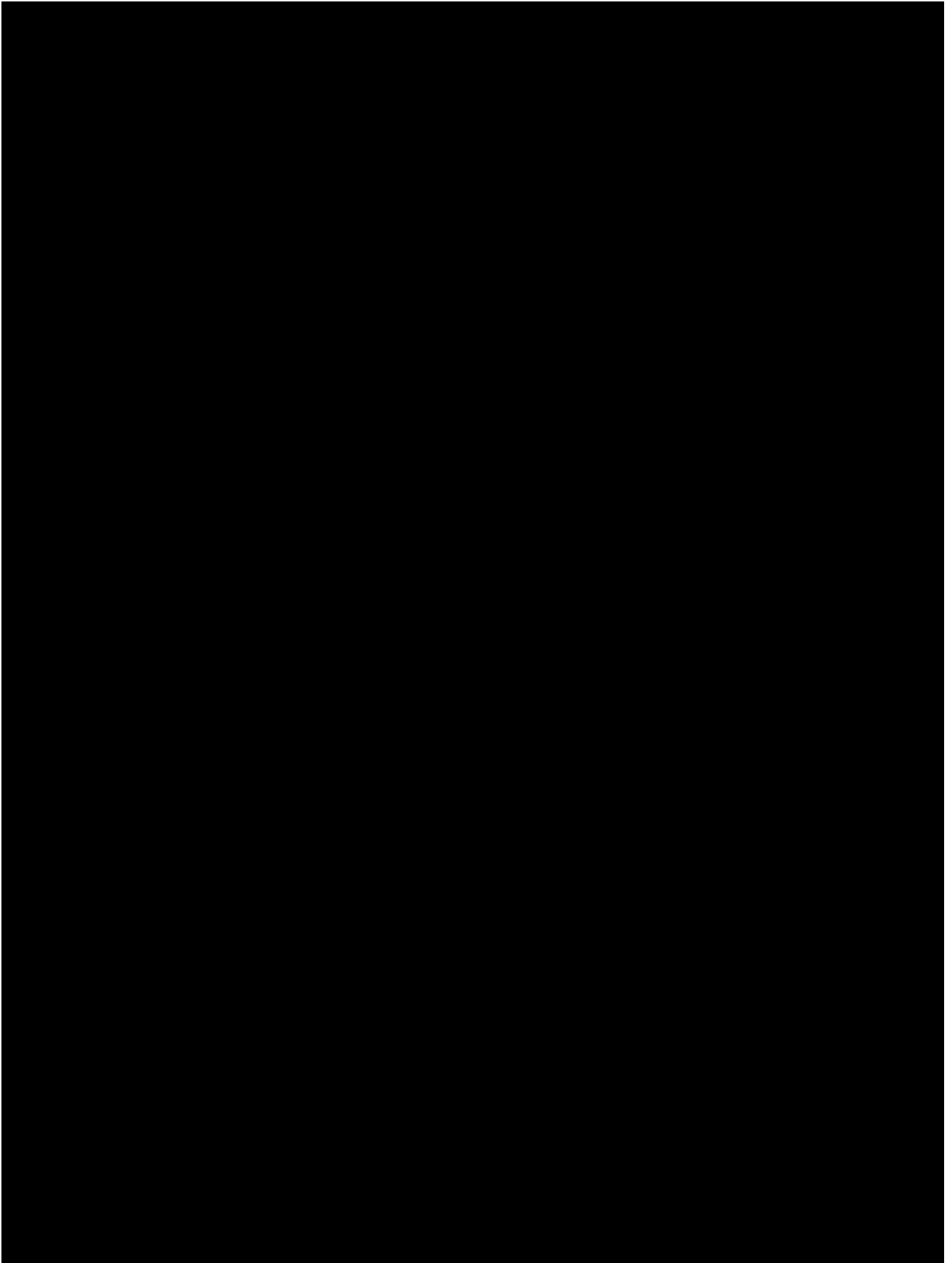


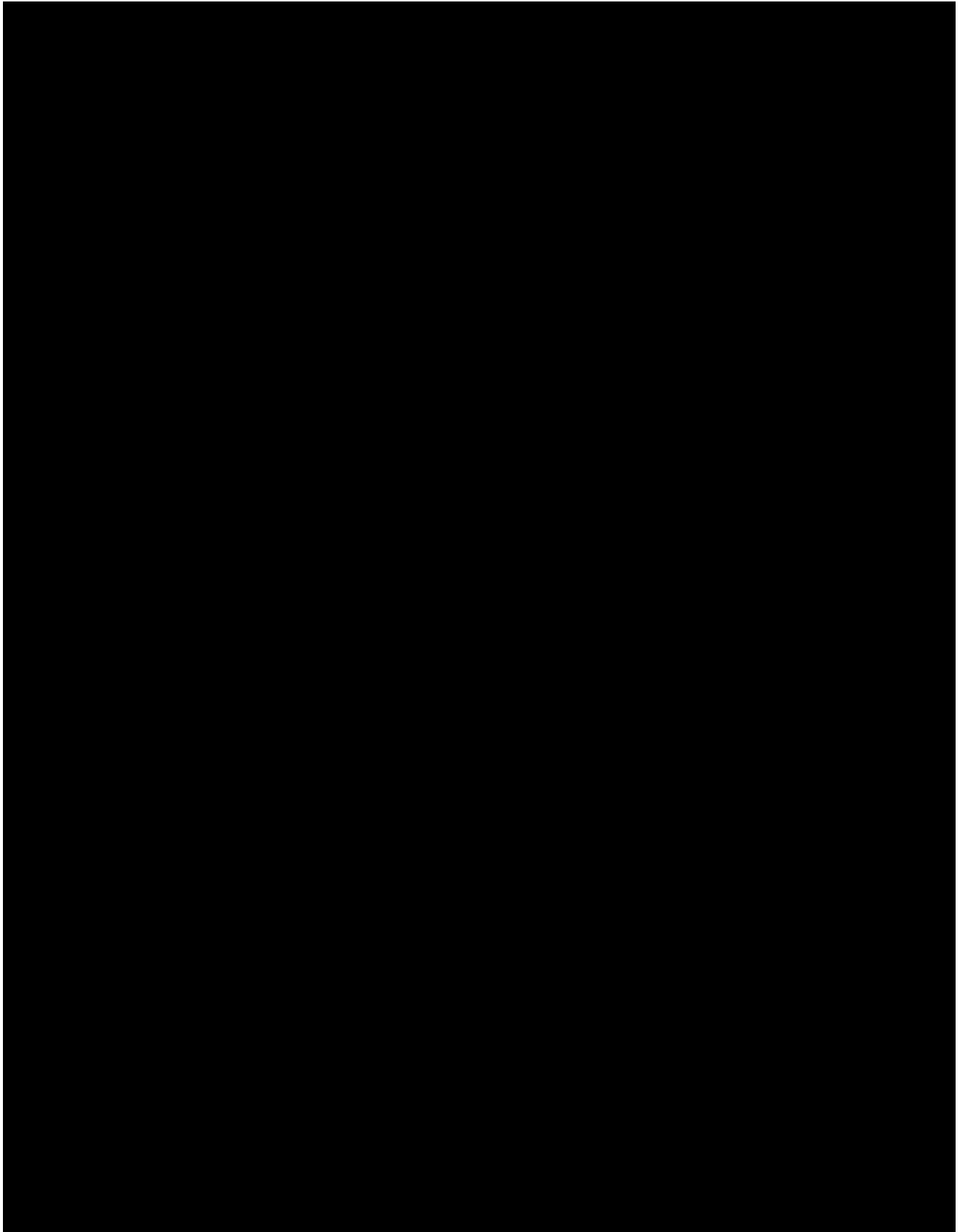


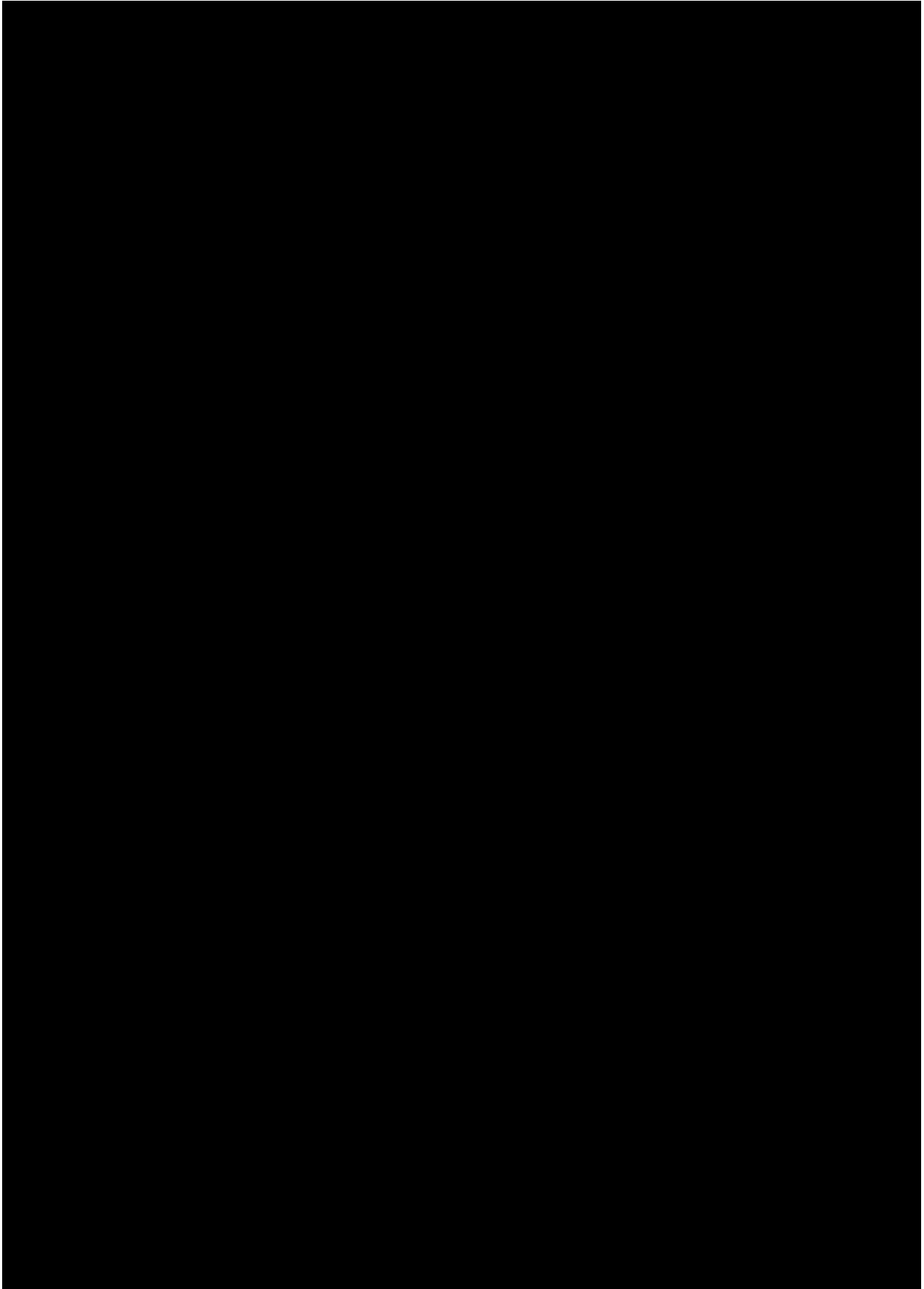


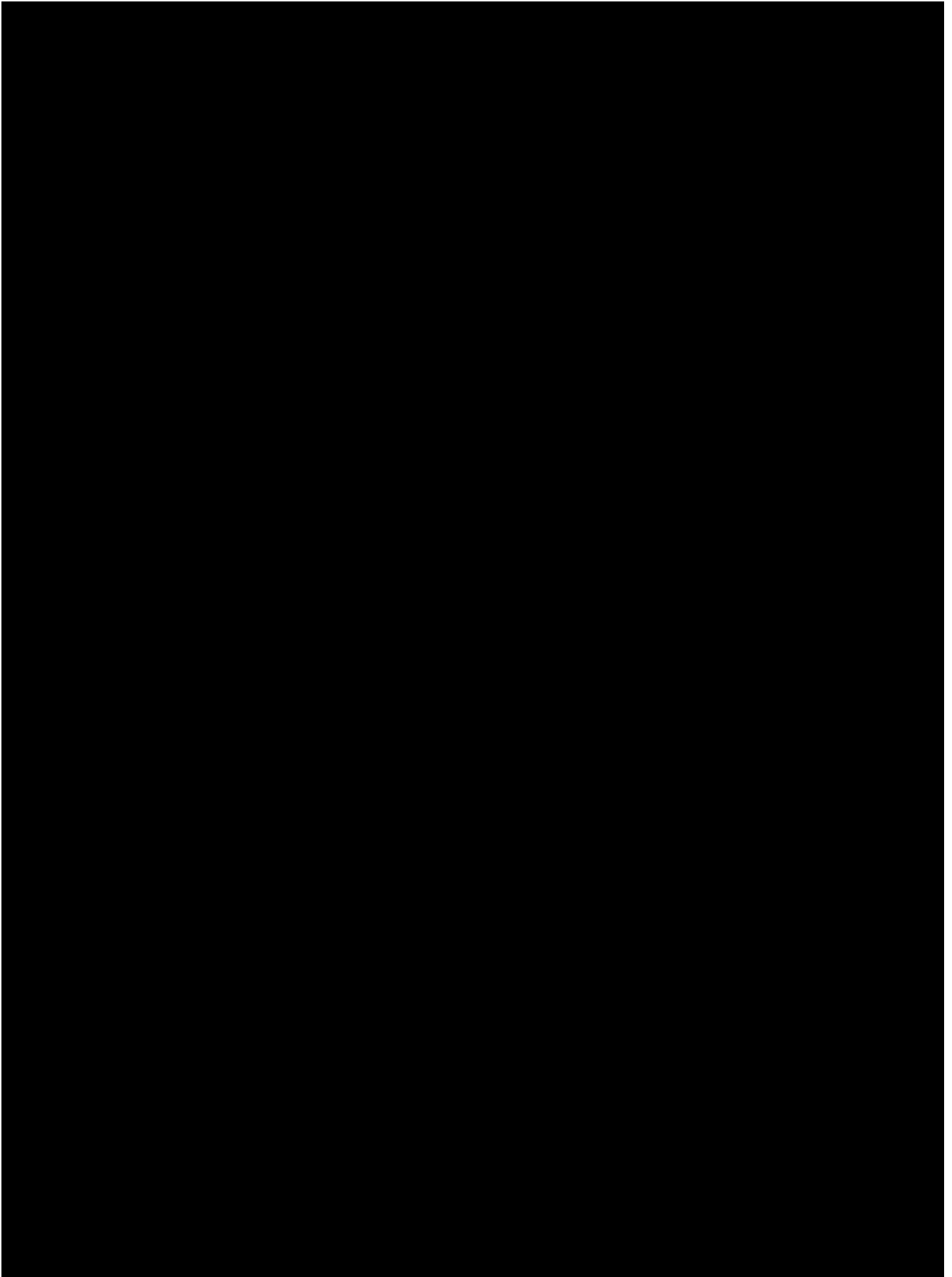


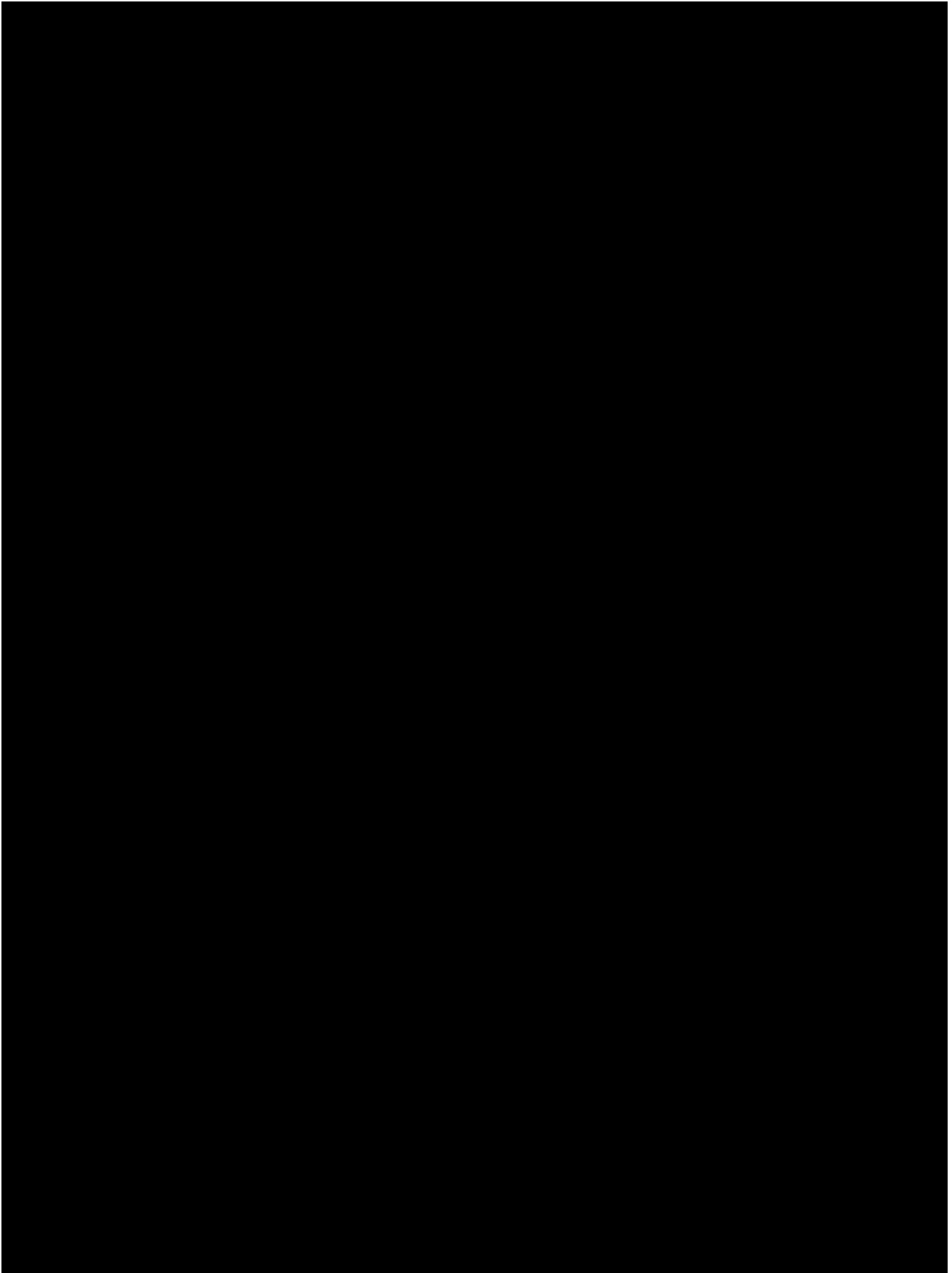


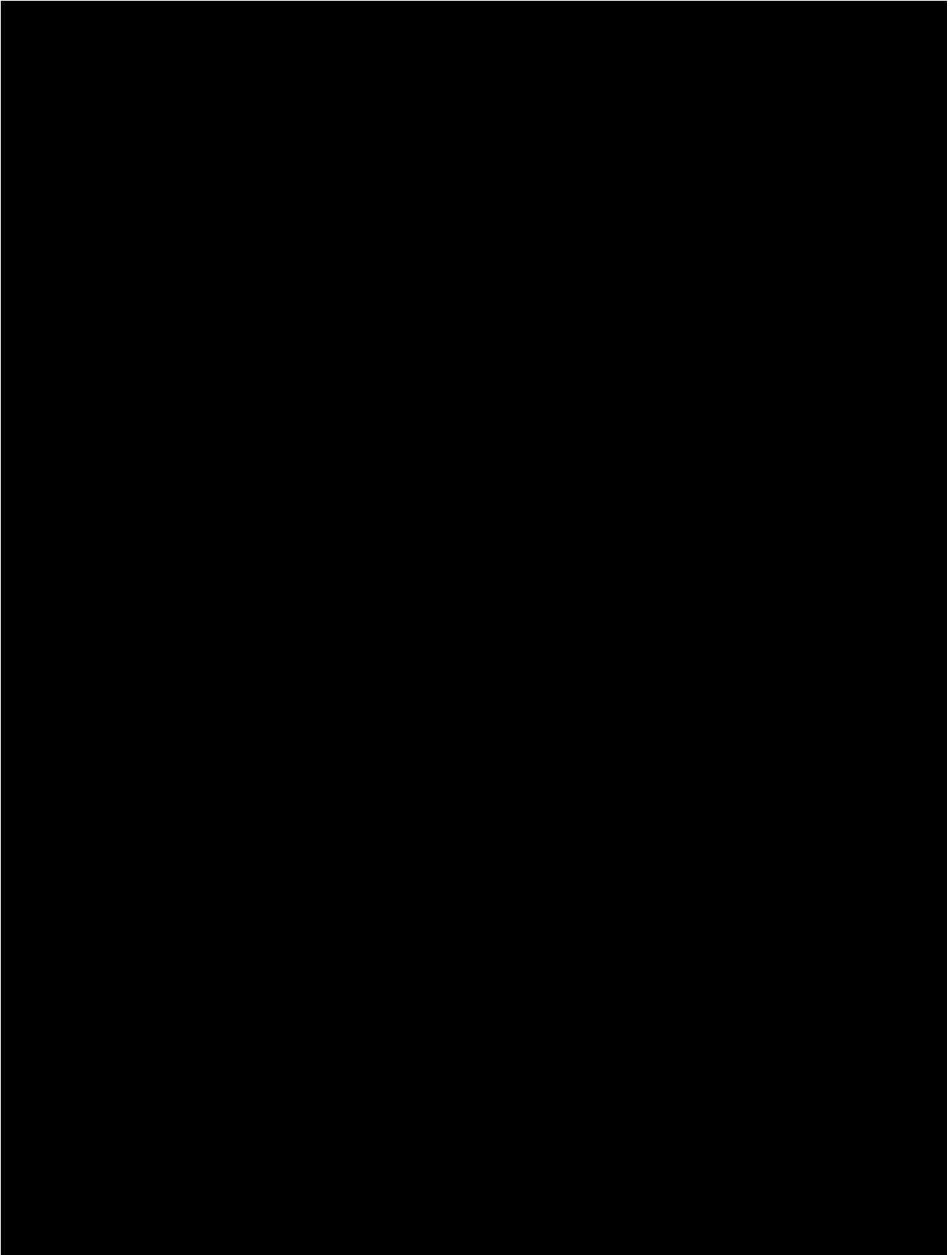


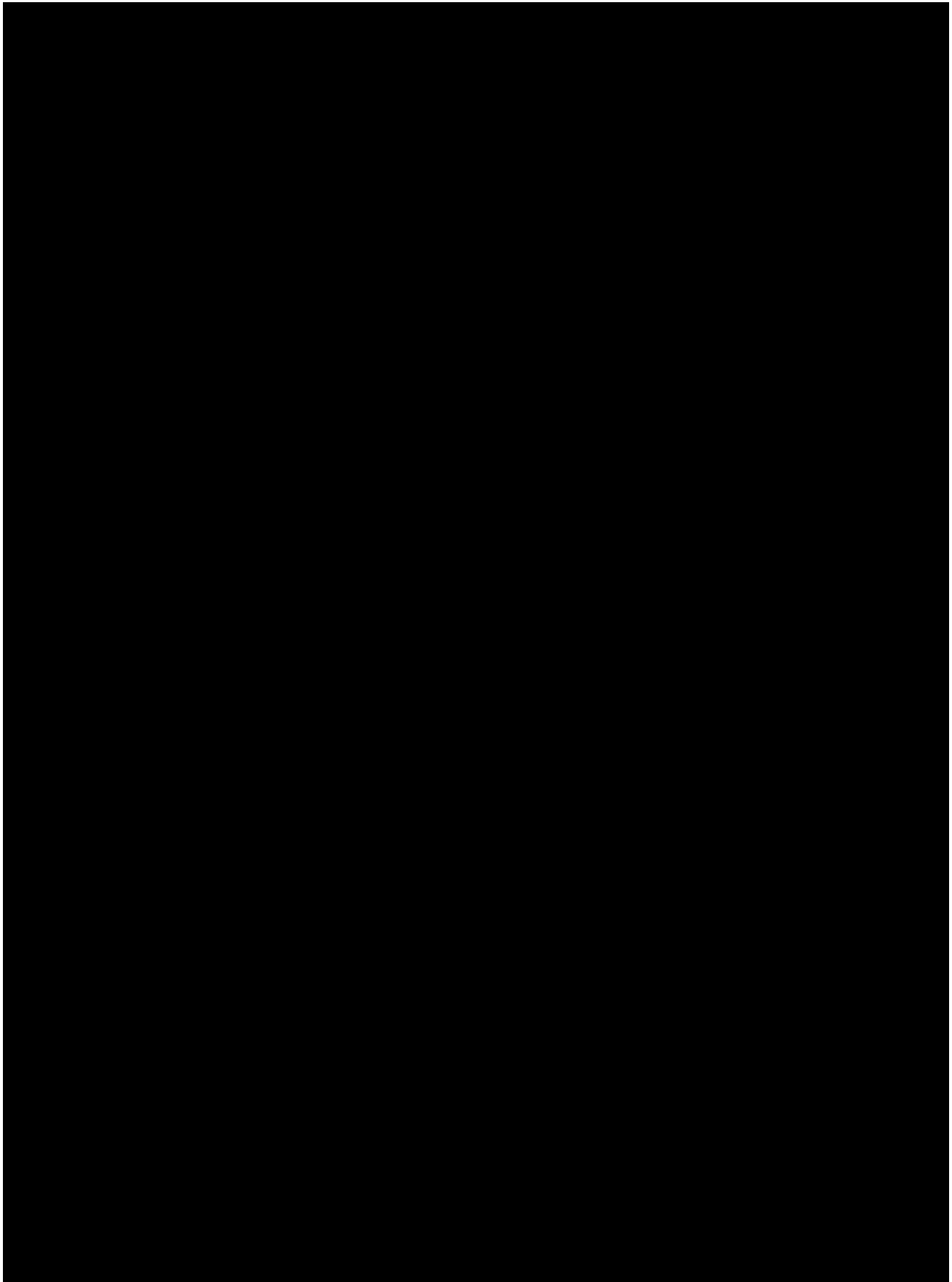


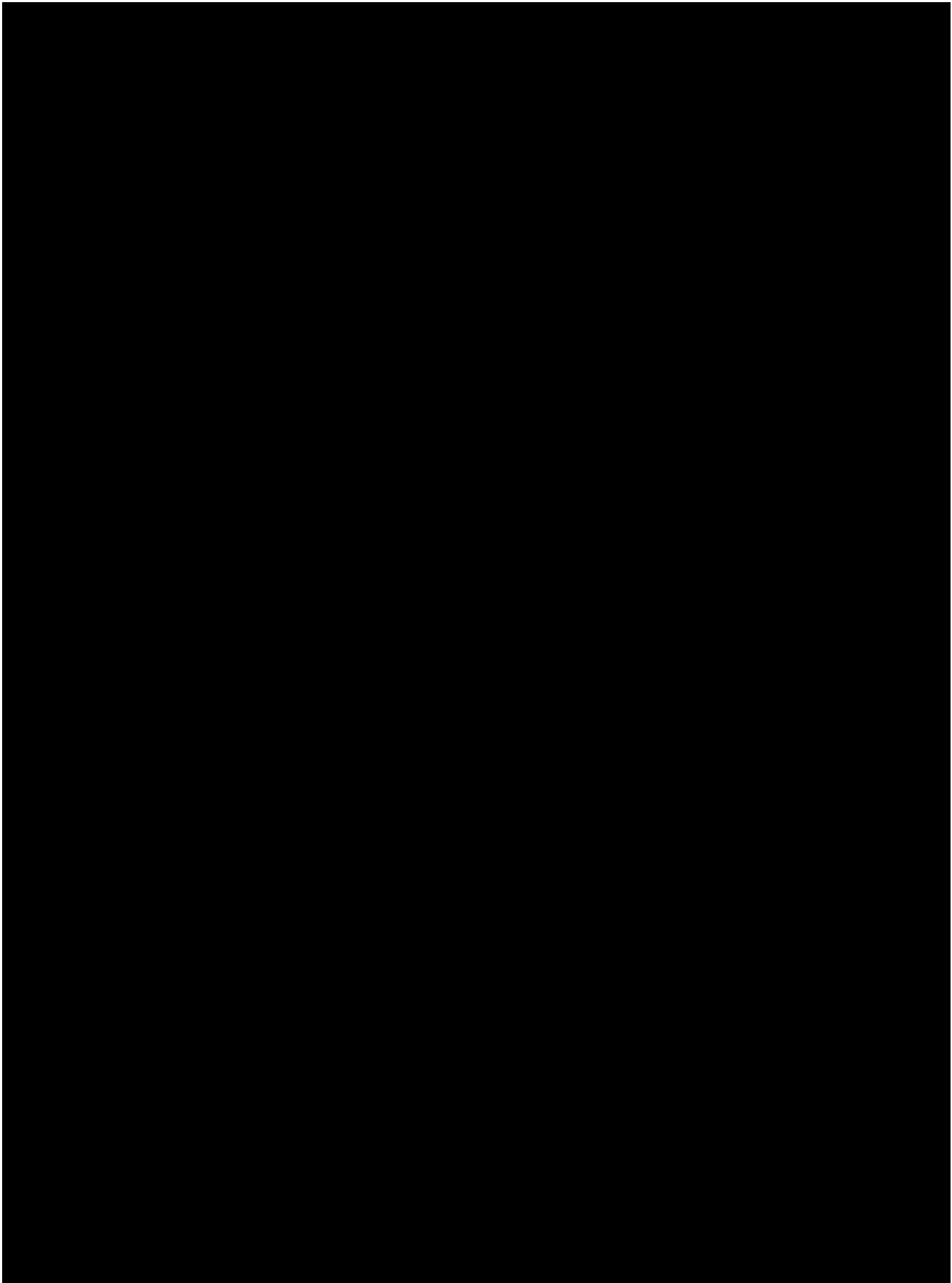


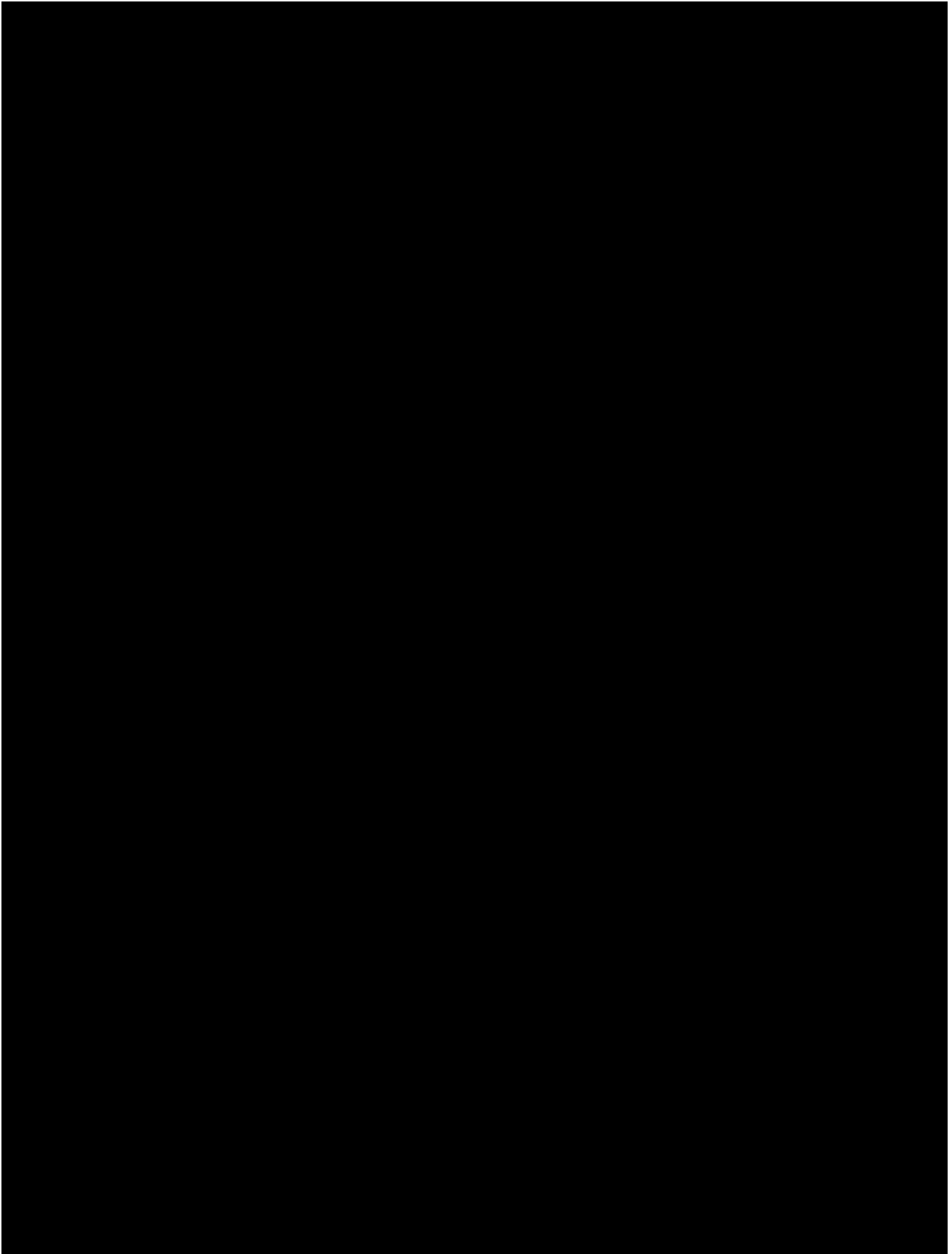


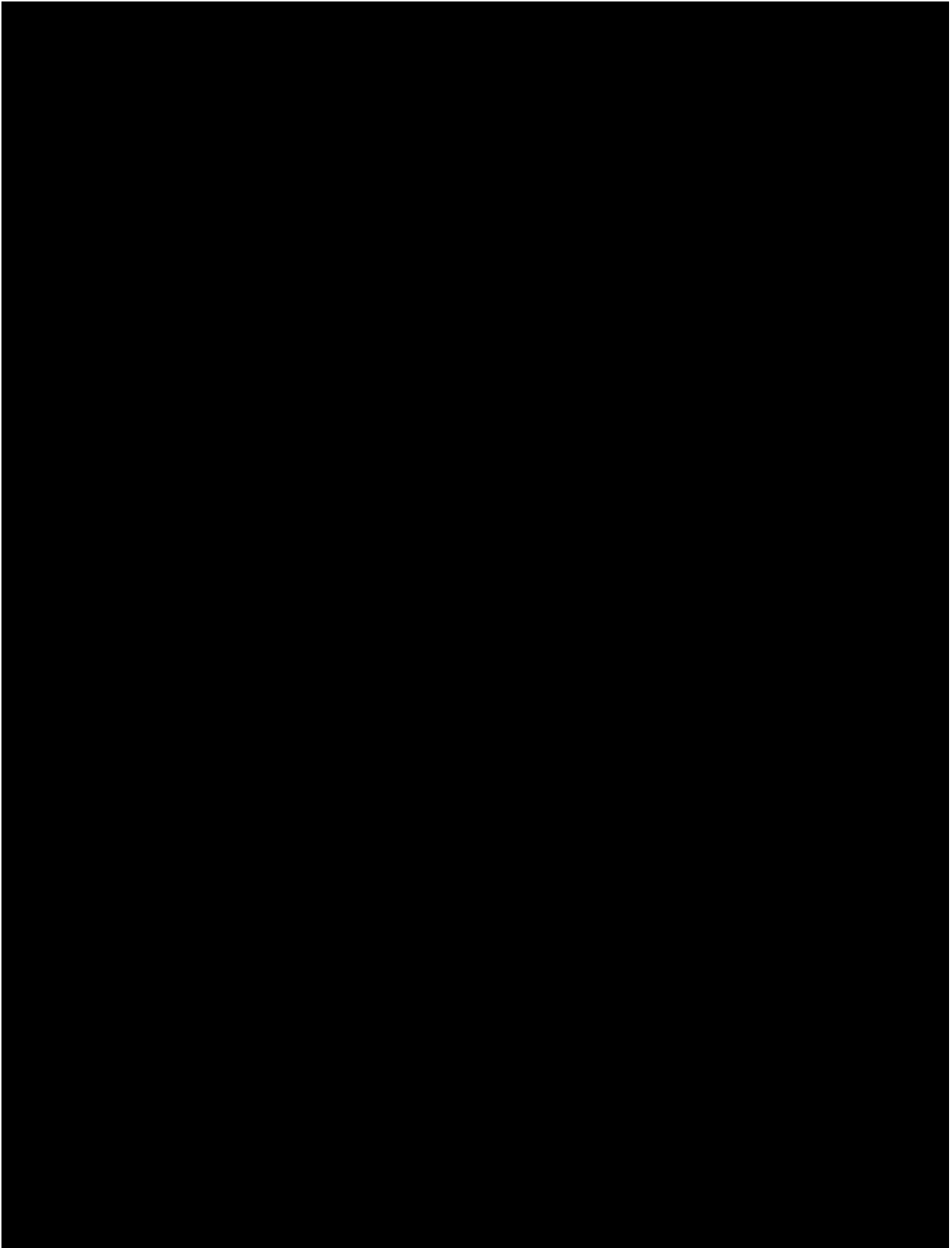


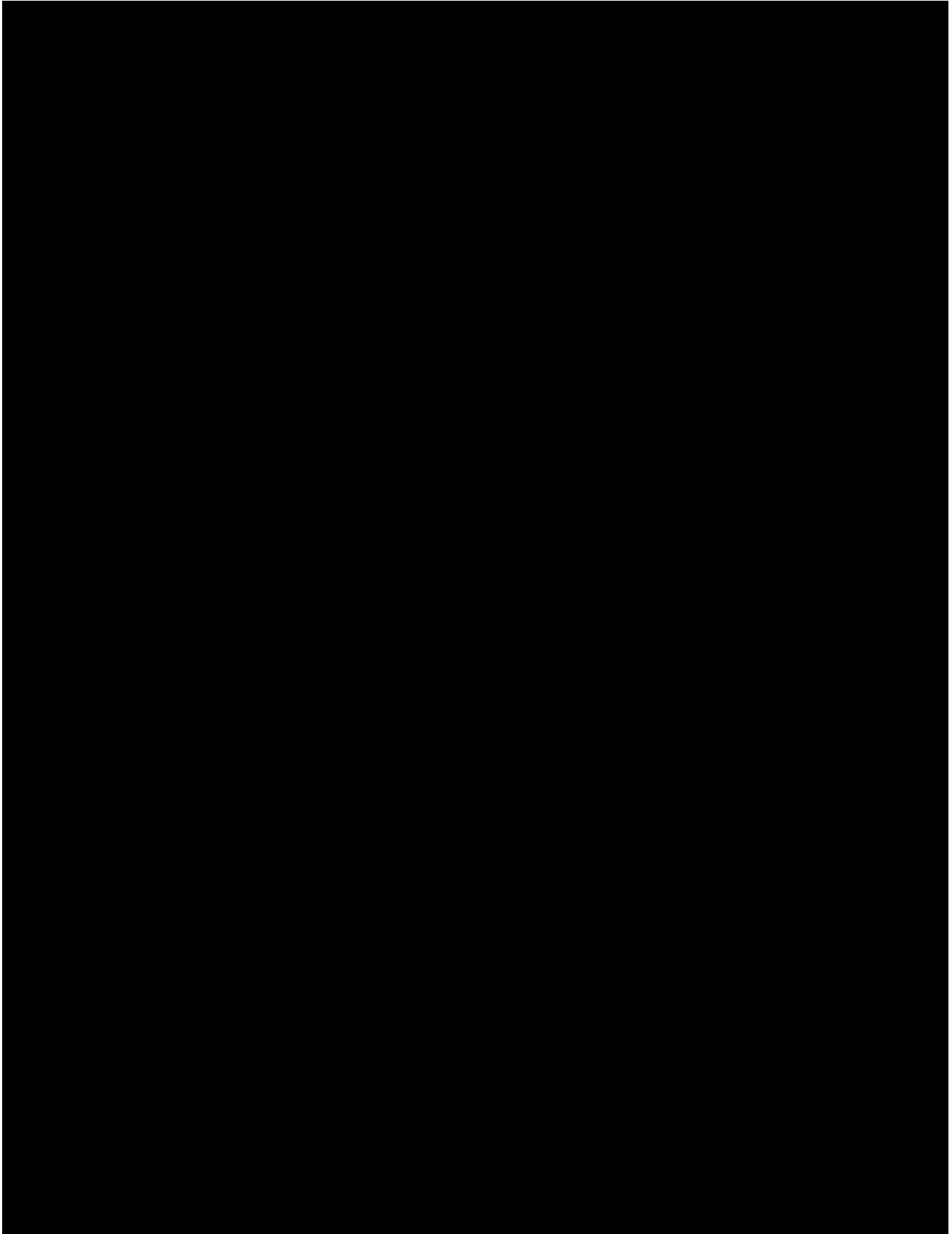


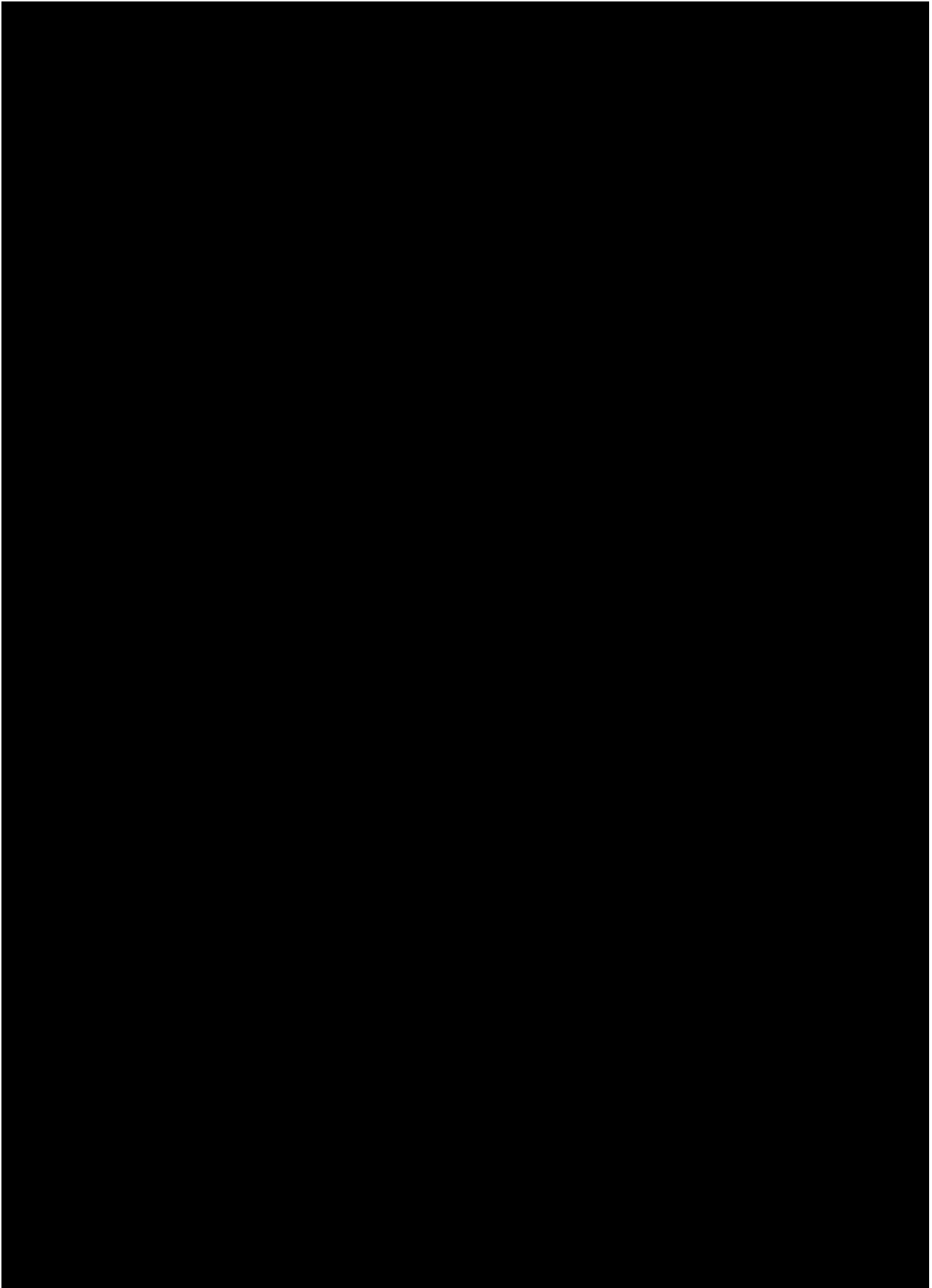


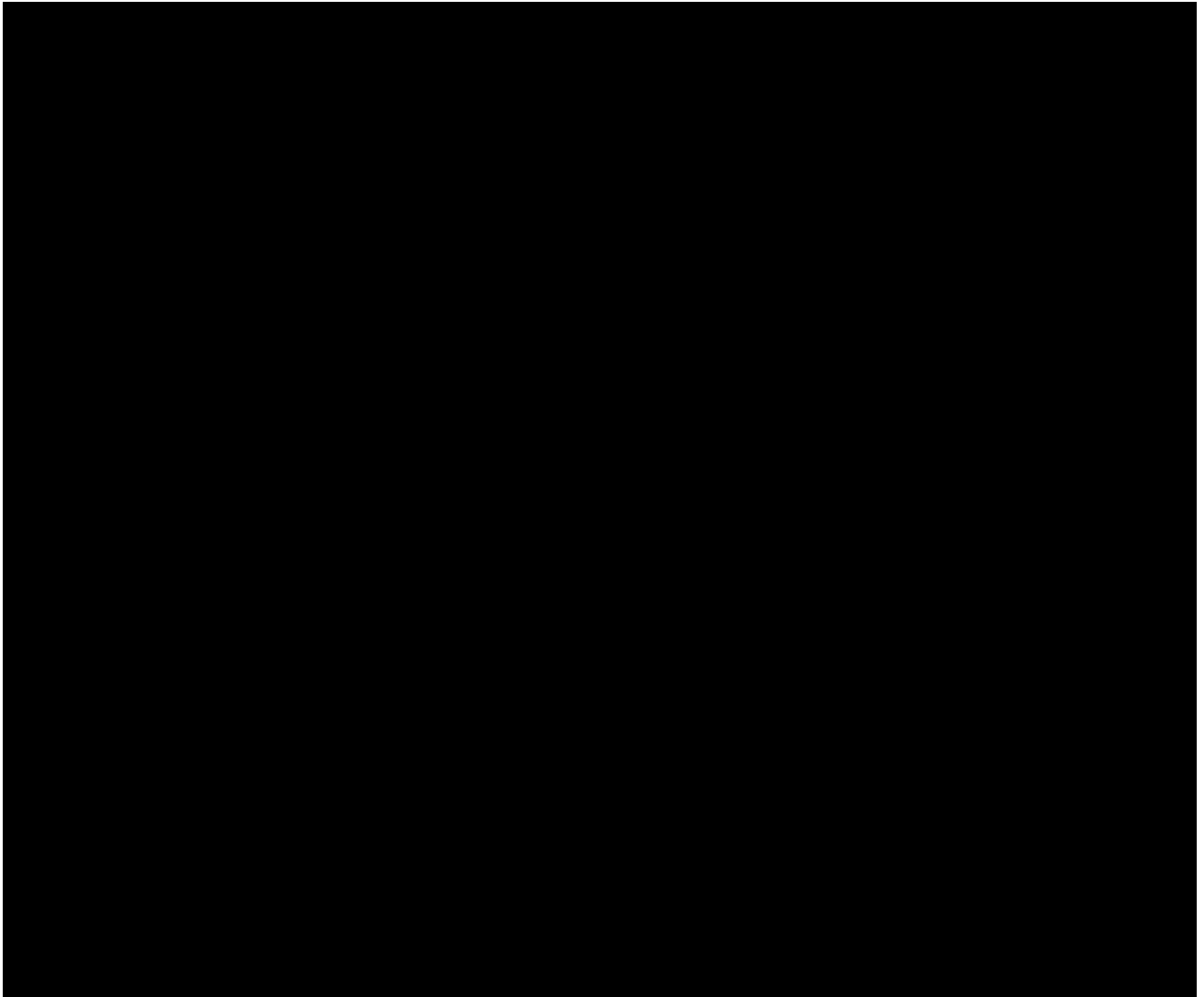








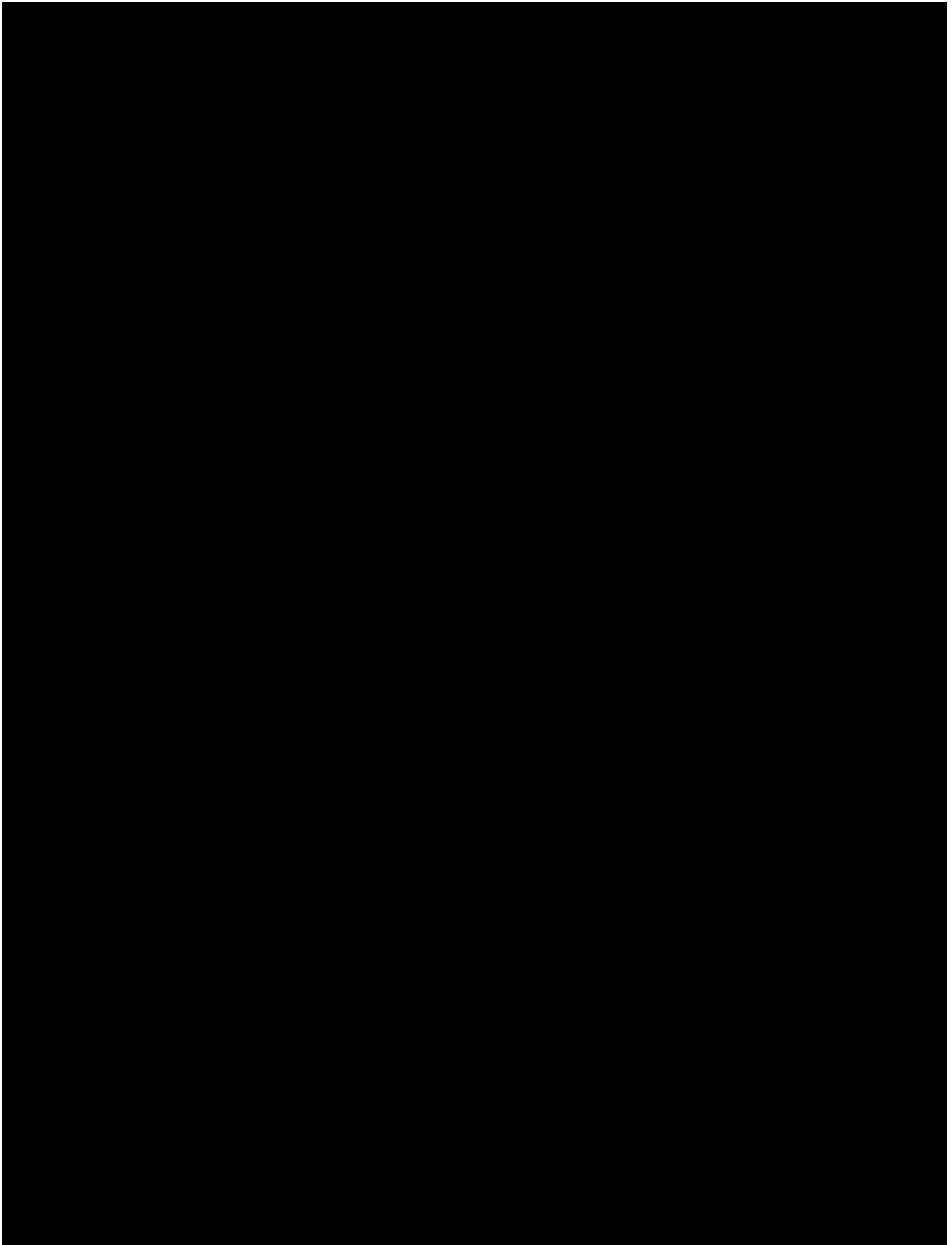


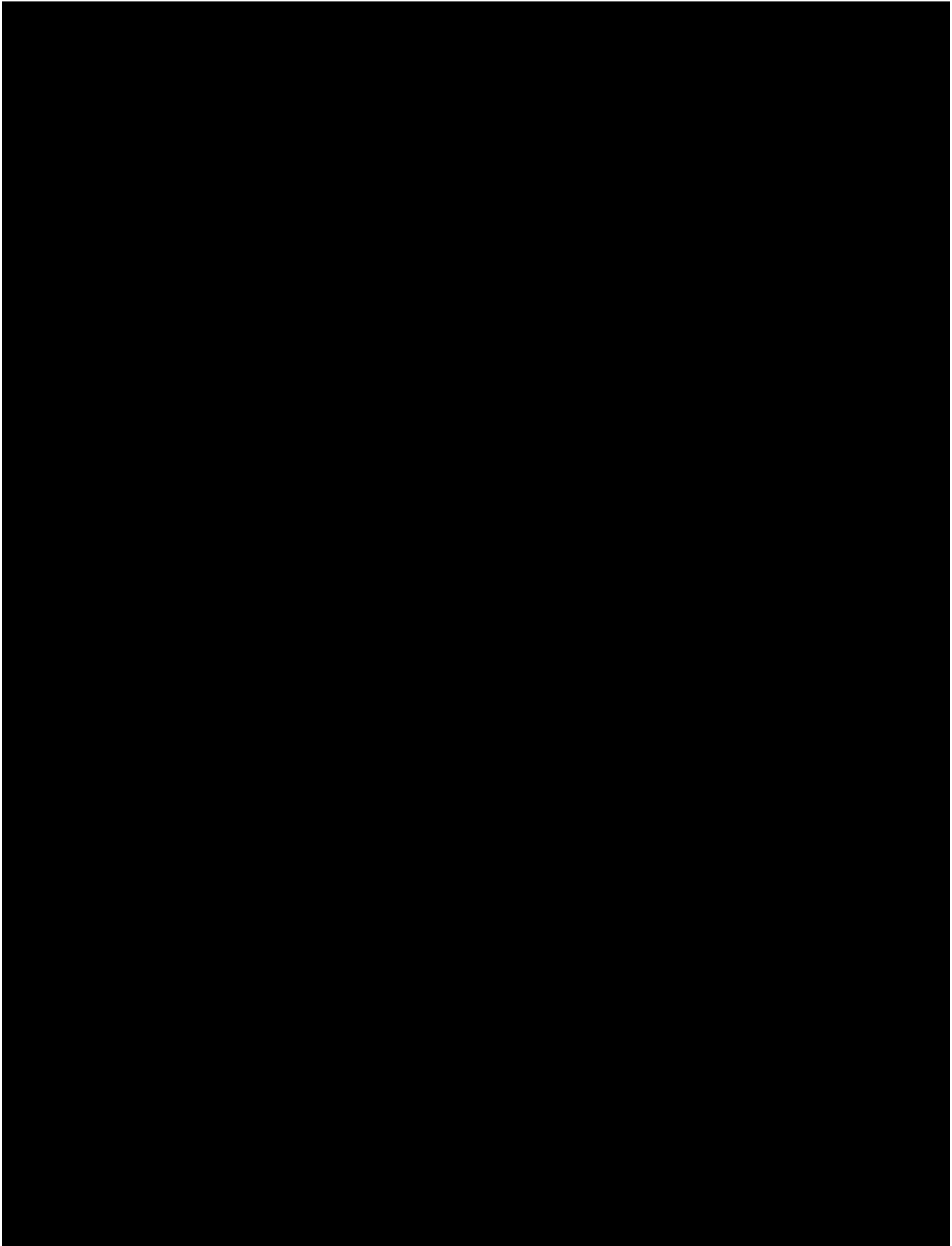


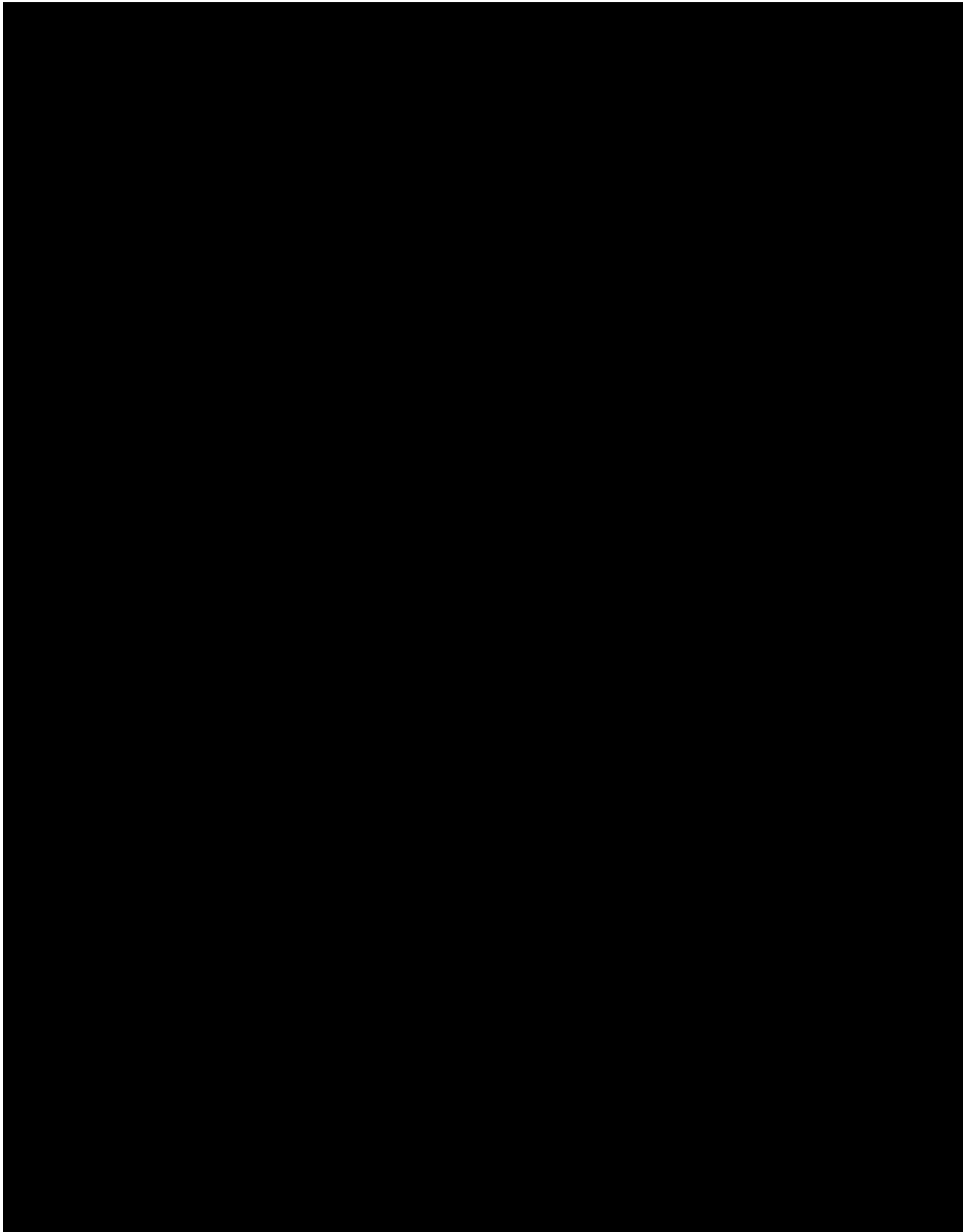
The following specifications concern specific tasks to be completed during the Contract term, which will be divided into the Project Execution Contract Phase and Operations and Maintenance (O&M) Contract Phase. This section also requests additional information about the Vendor's proposed Project and ongoing O&M support approach, including partnership with State IT and Business personnel for delivery. Awarded Vendor will complete delivery (defined as Agency acceptance of the stabilized solution) no later than September 30, 2024.

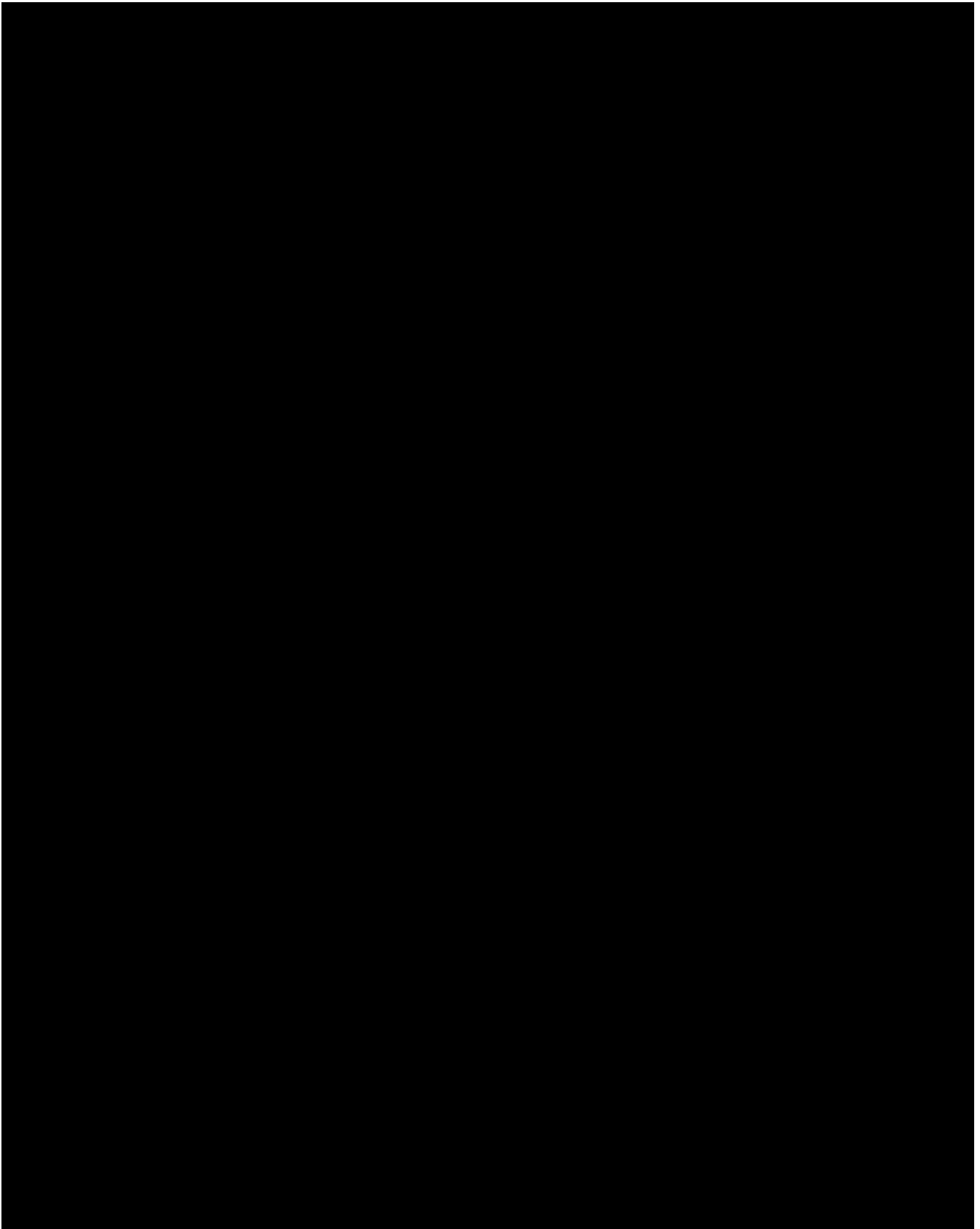
Describe the SDLC approach, methodology, and tools you will use for supporting the Agency in delivering the proposed Solution, including Changes made to the Solution. The Agency requests use of agile-based methodologies.

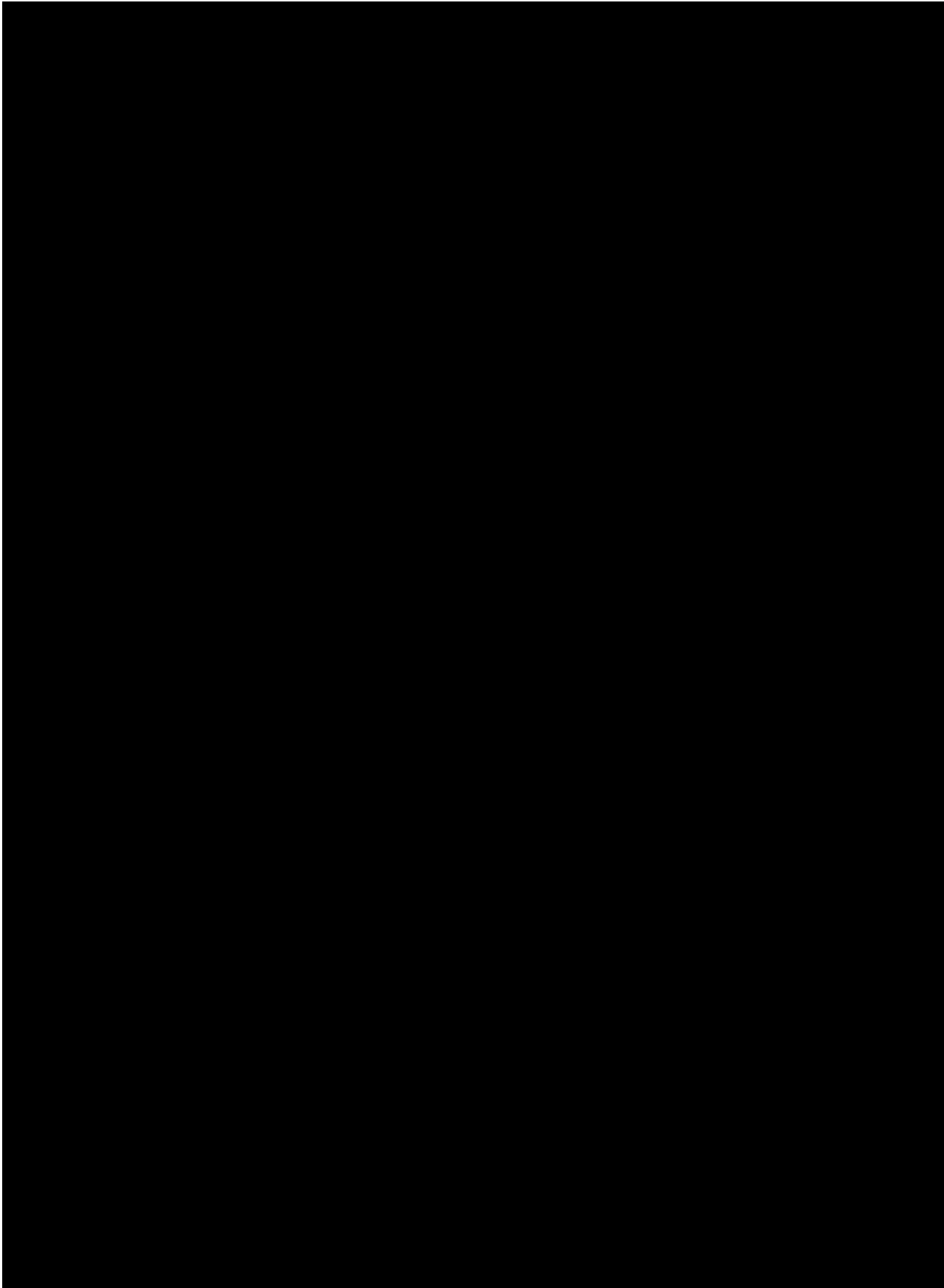
[illegible]

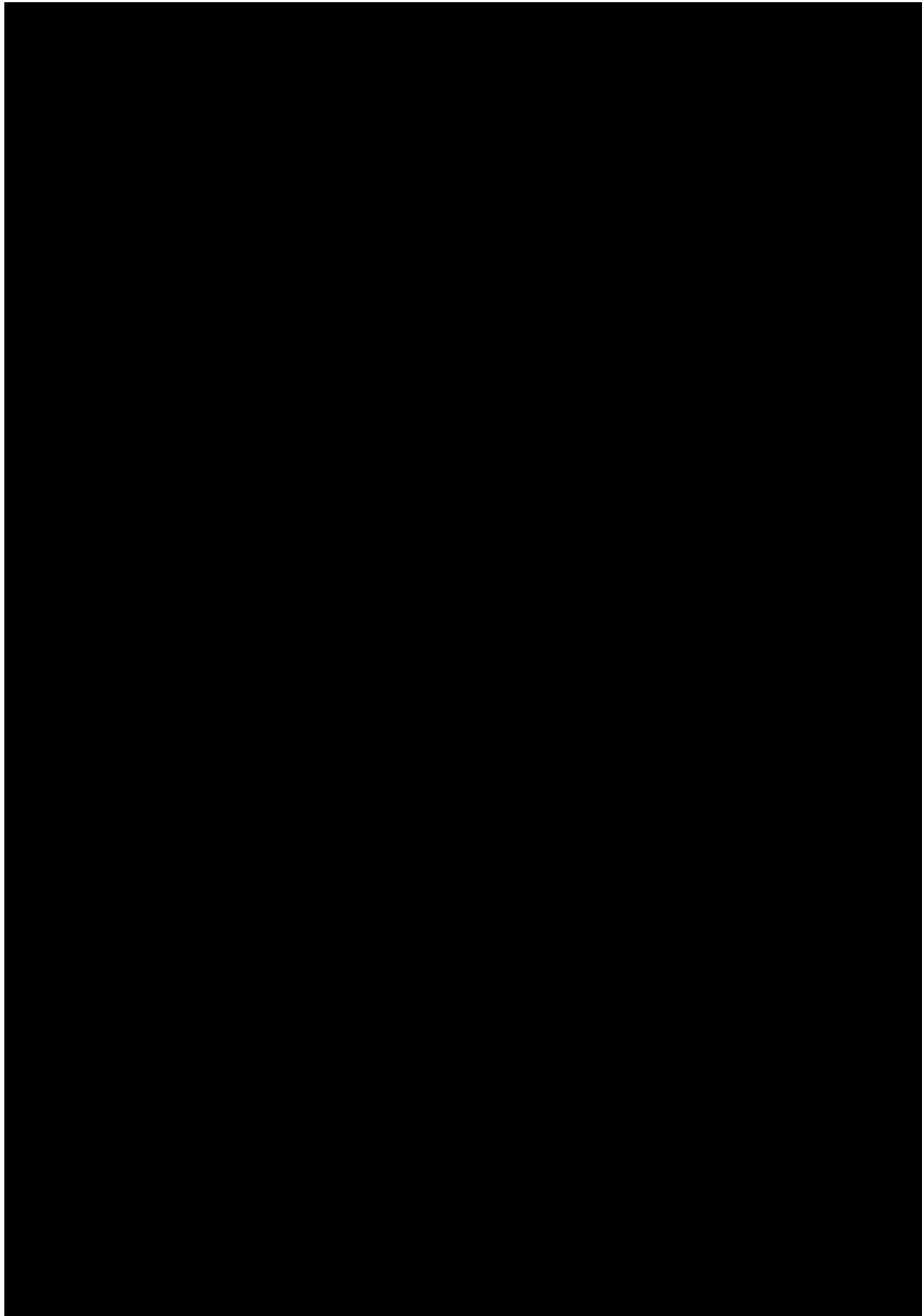


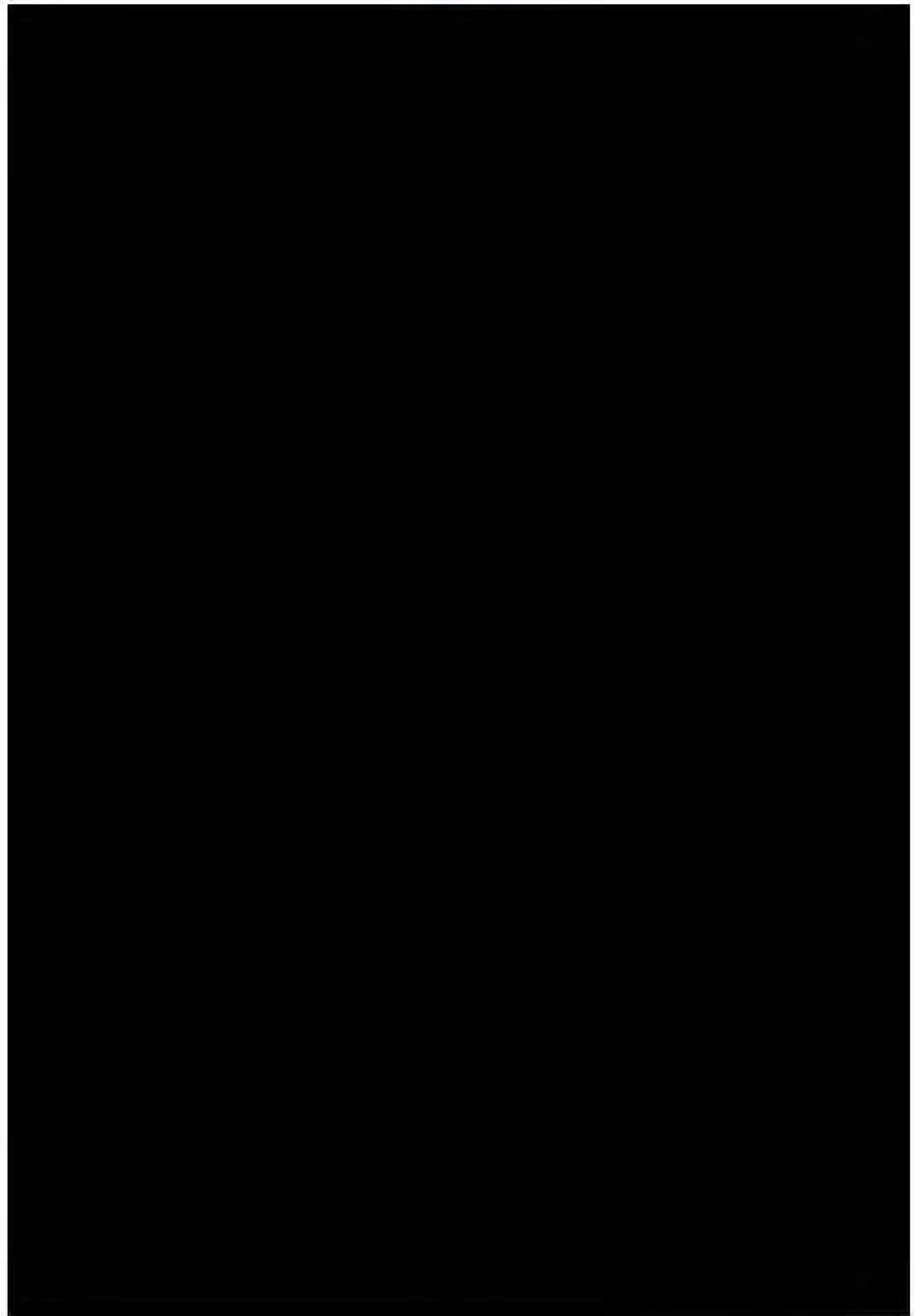


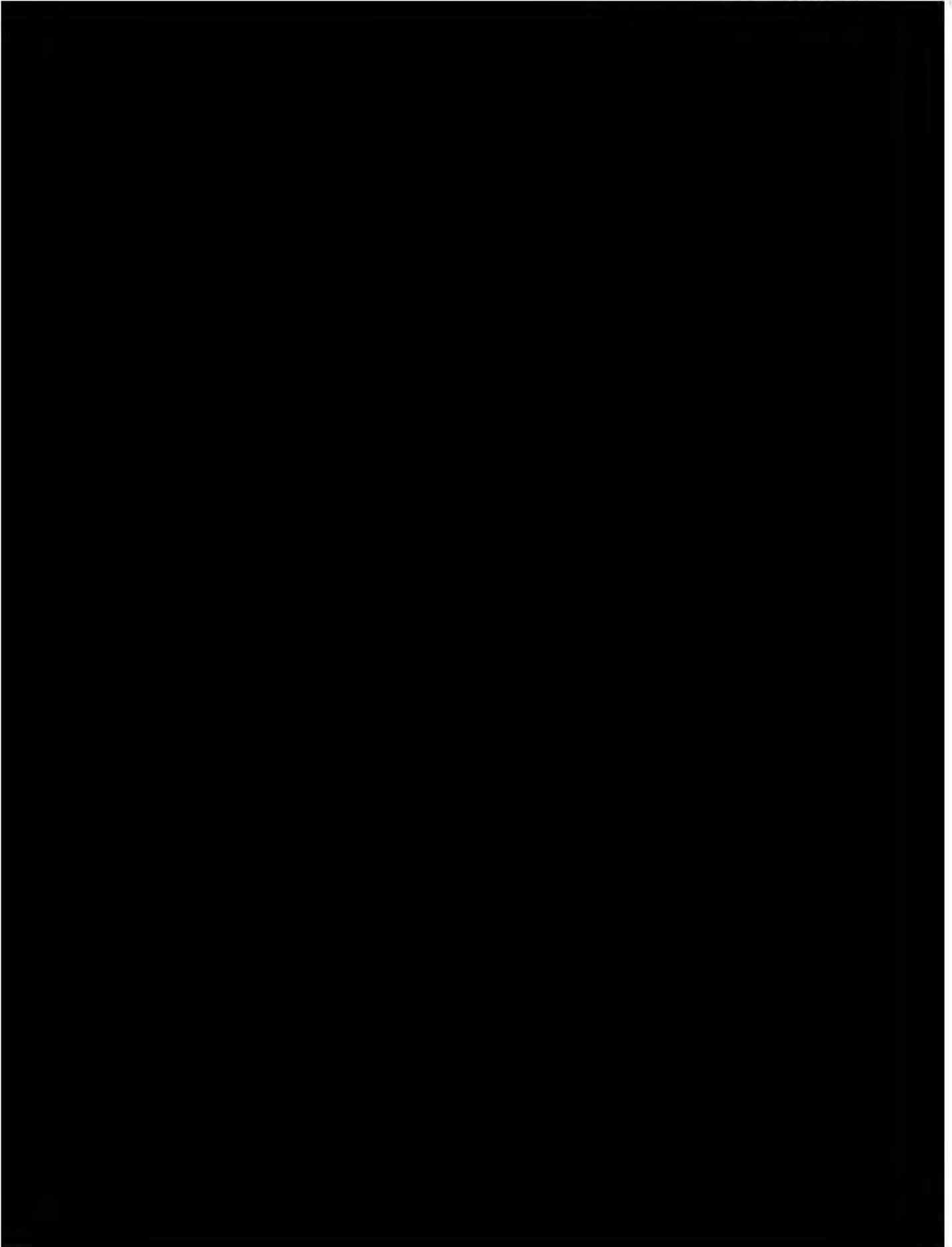


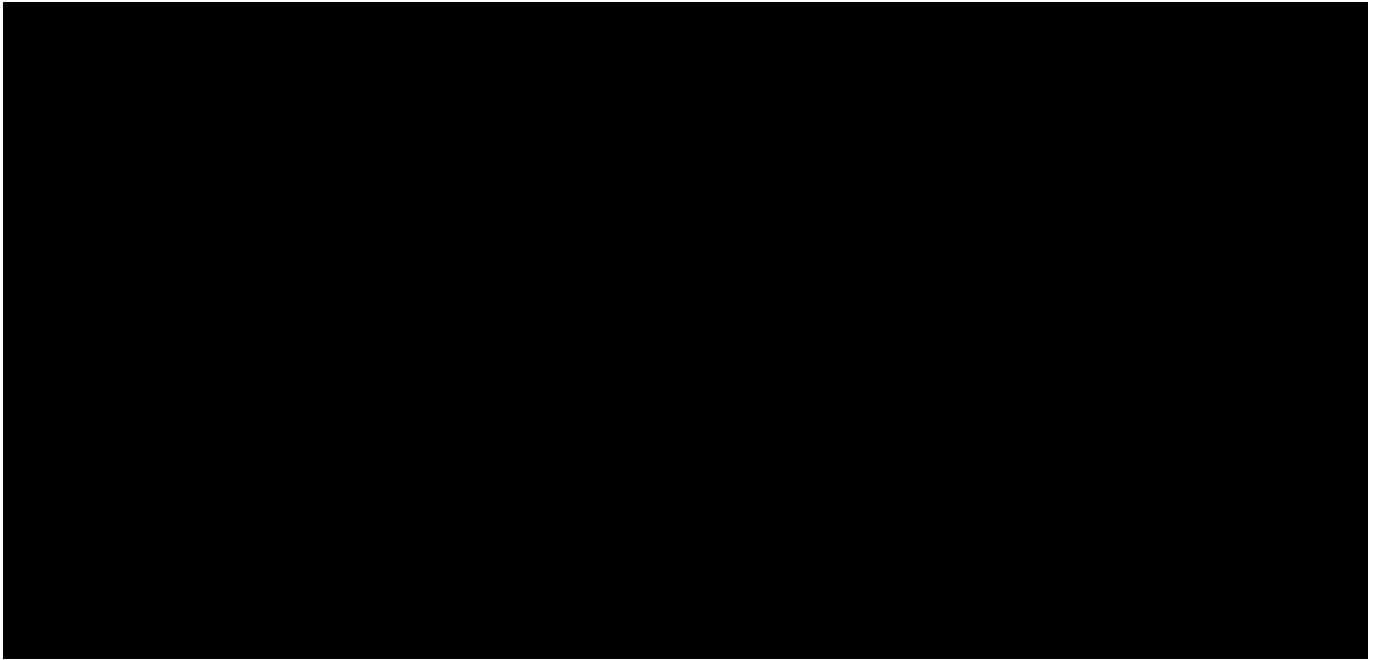










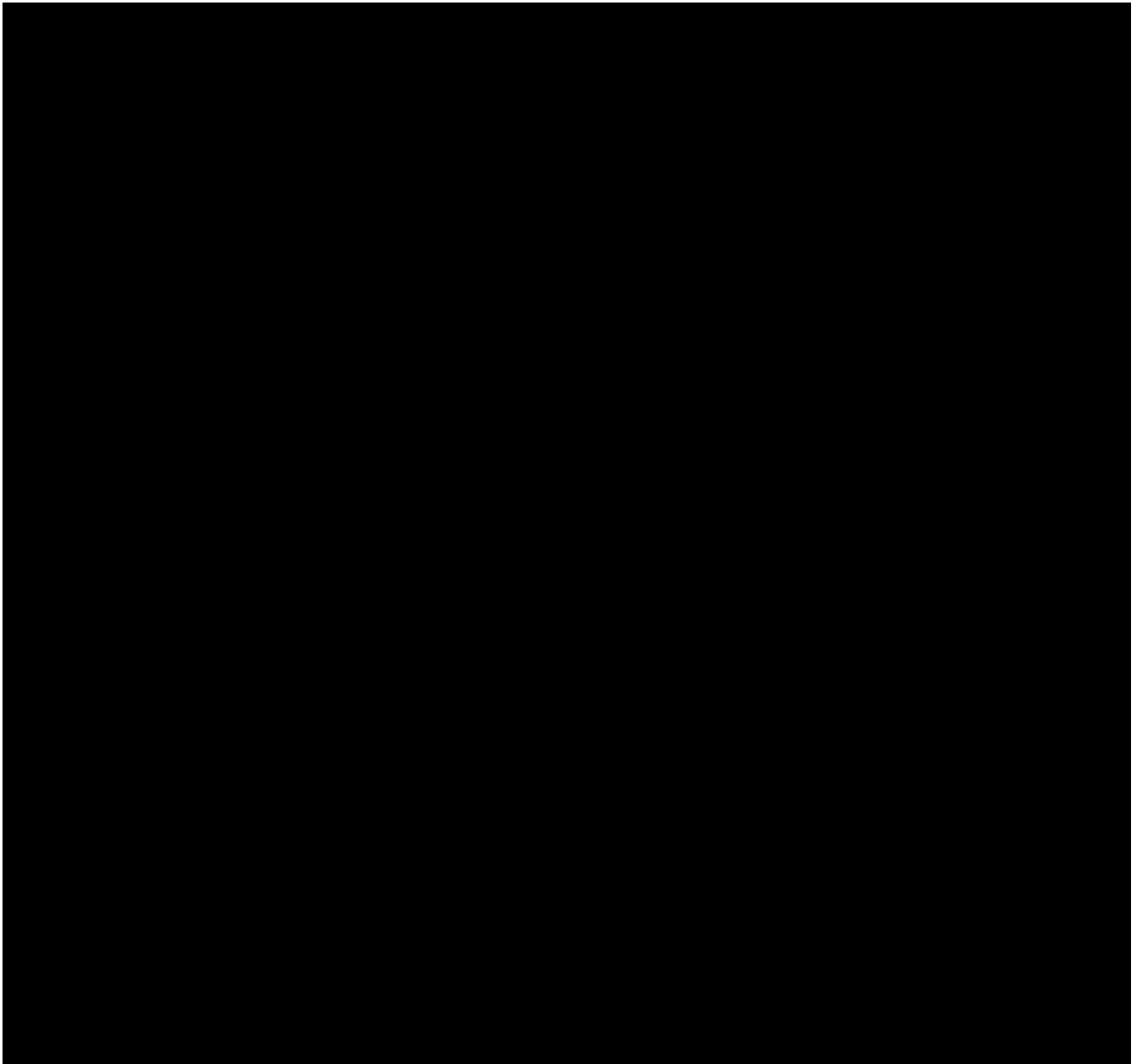


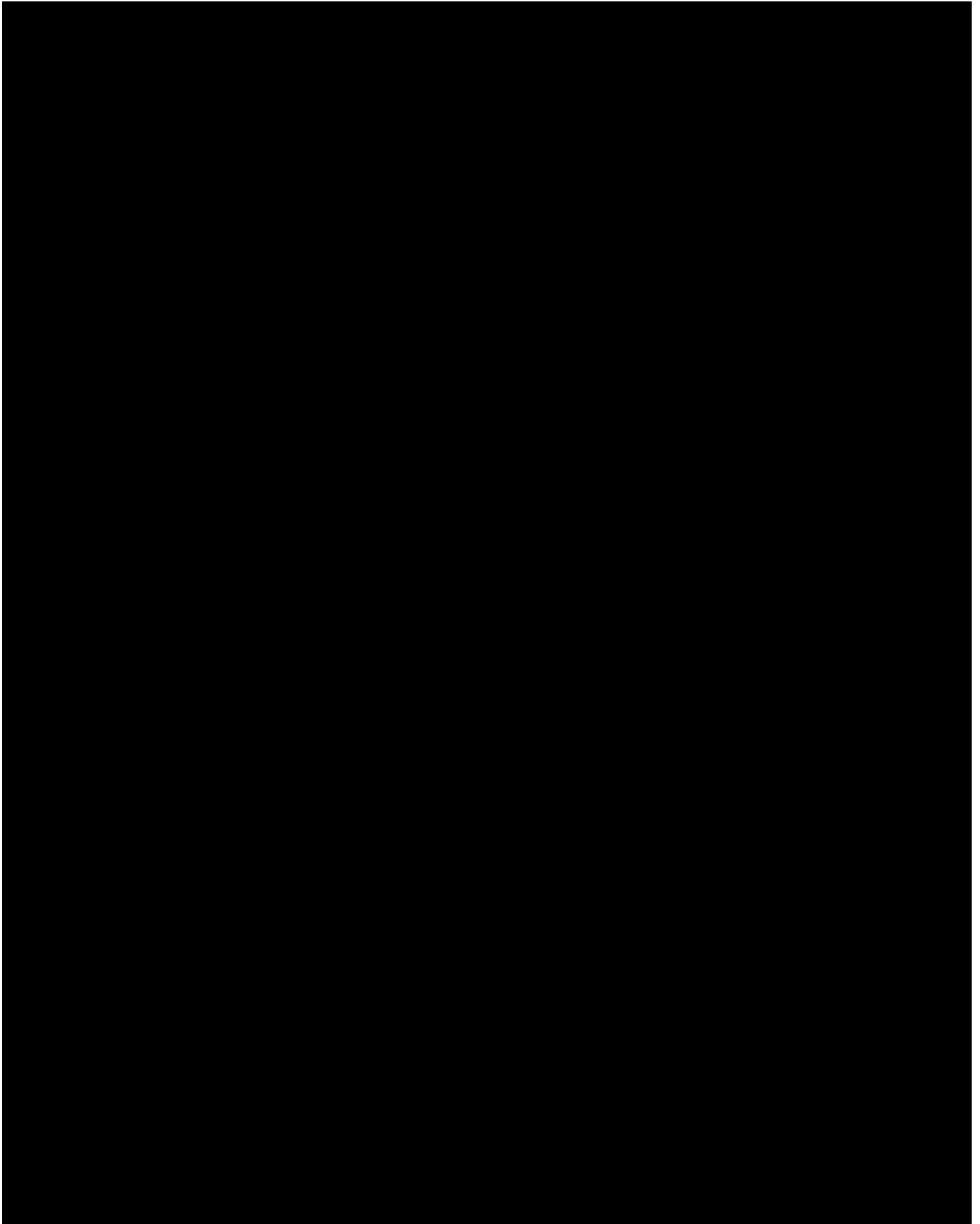
3.5.2 Project Management

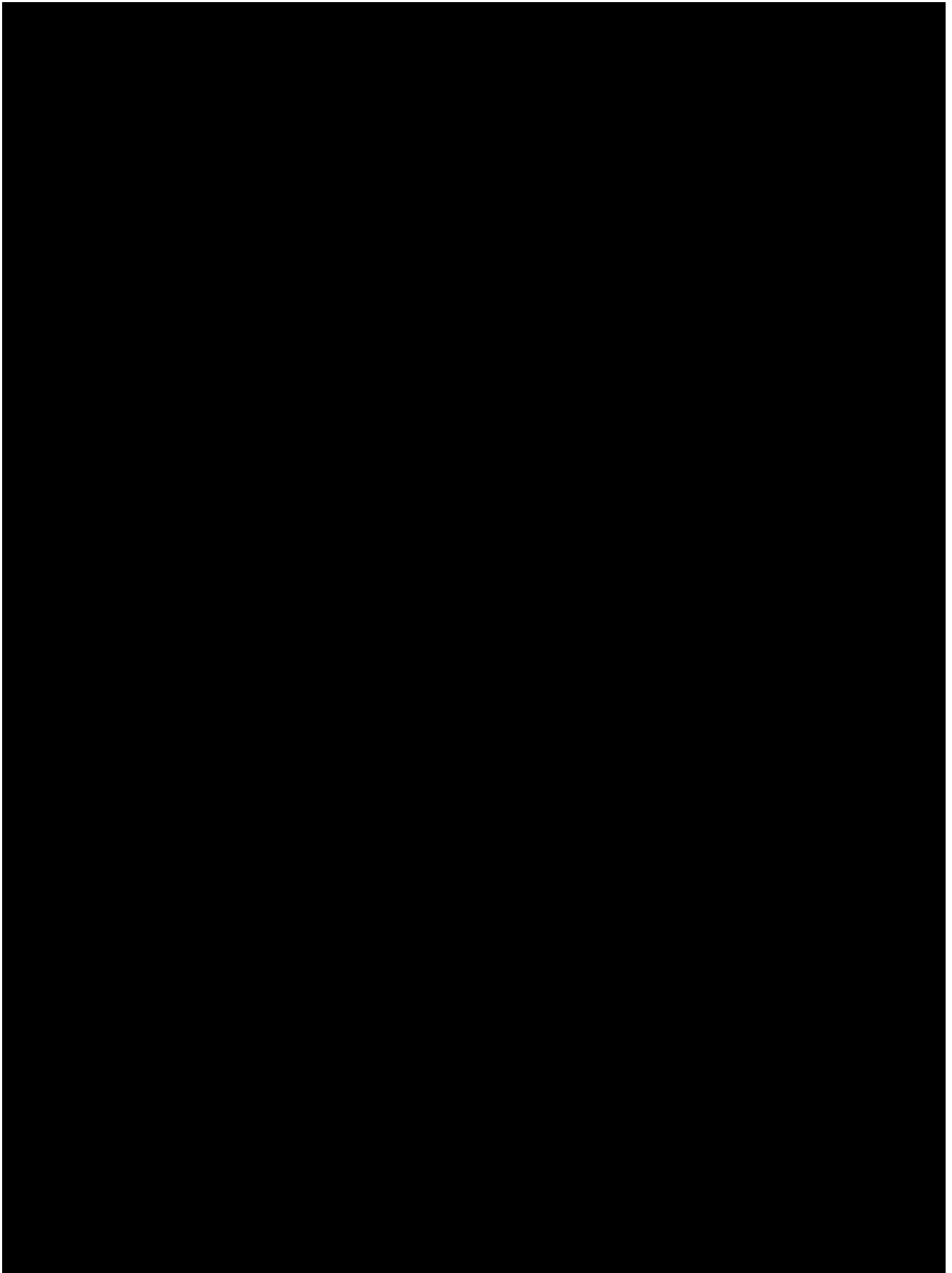
1. Vendor Project Management Approach

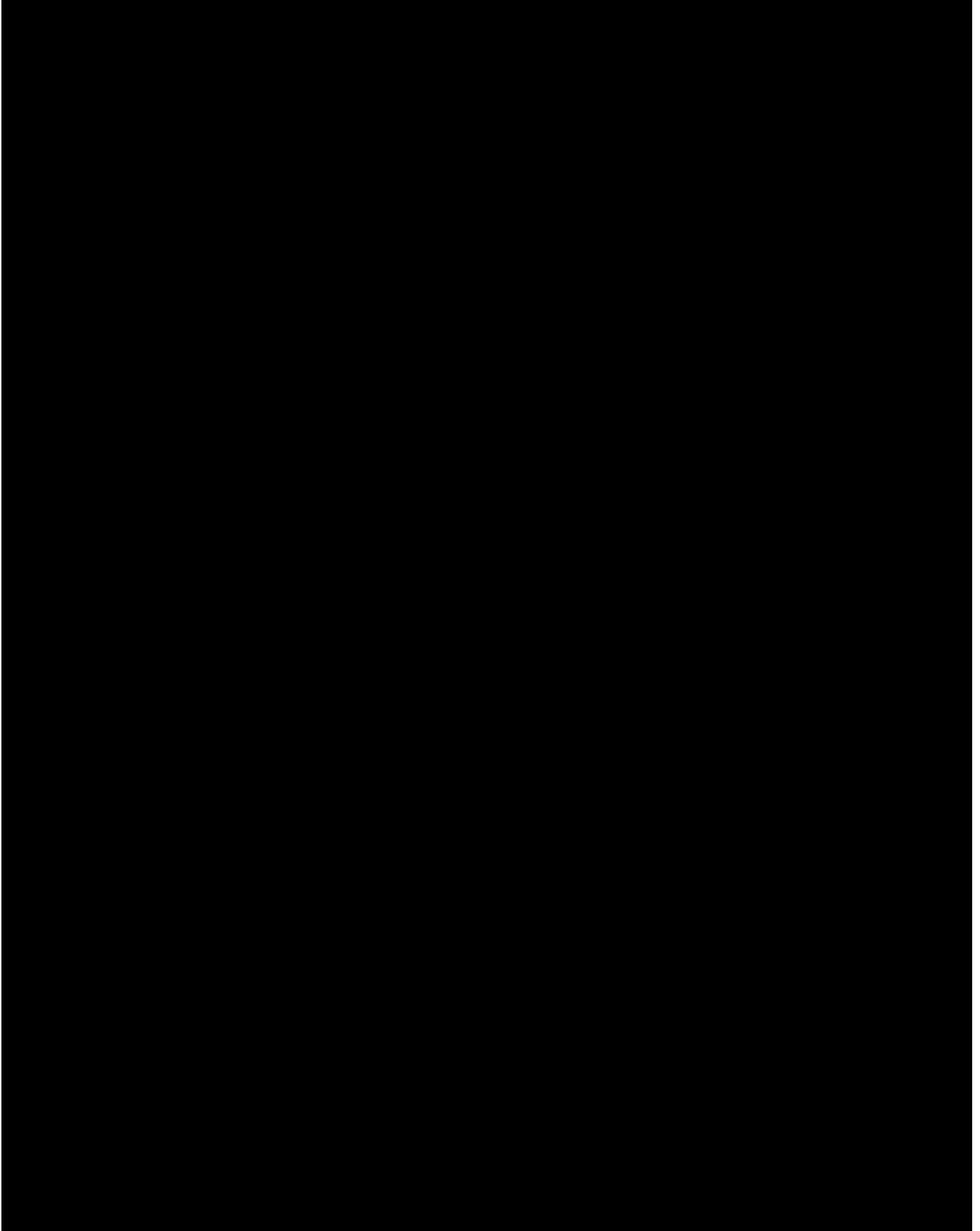
The State's framework employs decision points throughout the project for approval to proceed with next tasks (reference <https://it.nc.gov/programs/project-portfolio-management/quality-management-system>). The project stages in which the Vendor will be engaged include the Planning and Design Phase, Execution and Build, Implementation and Closeout phases. Reference Section 7.11 for additional information about Project Management. Describe your approach to Project Management to be utilized in support of the State's project management framework, including:

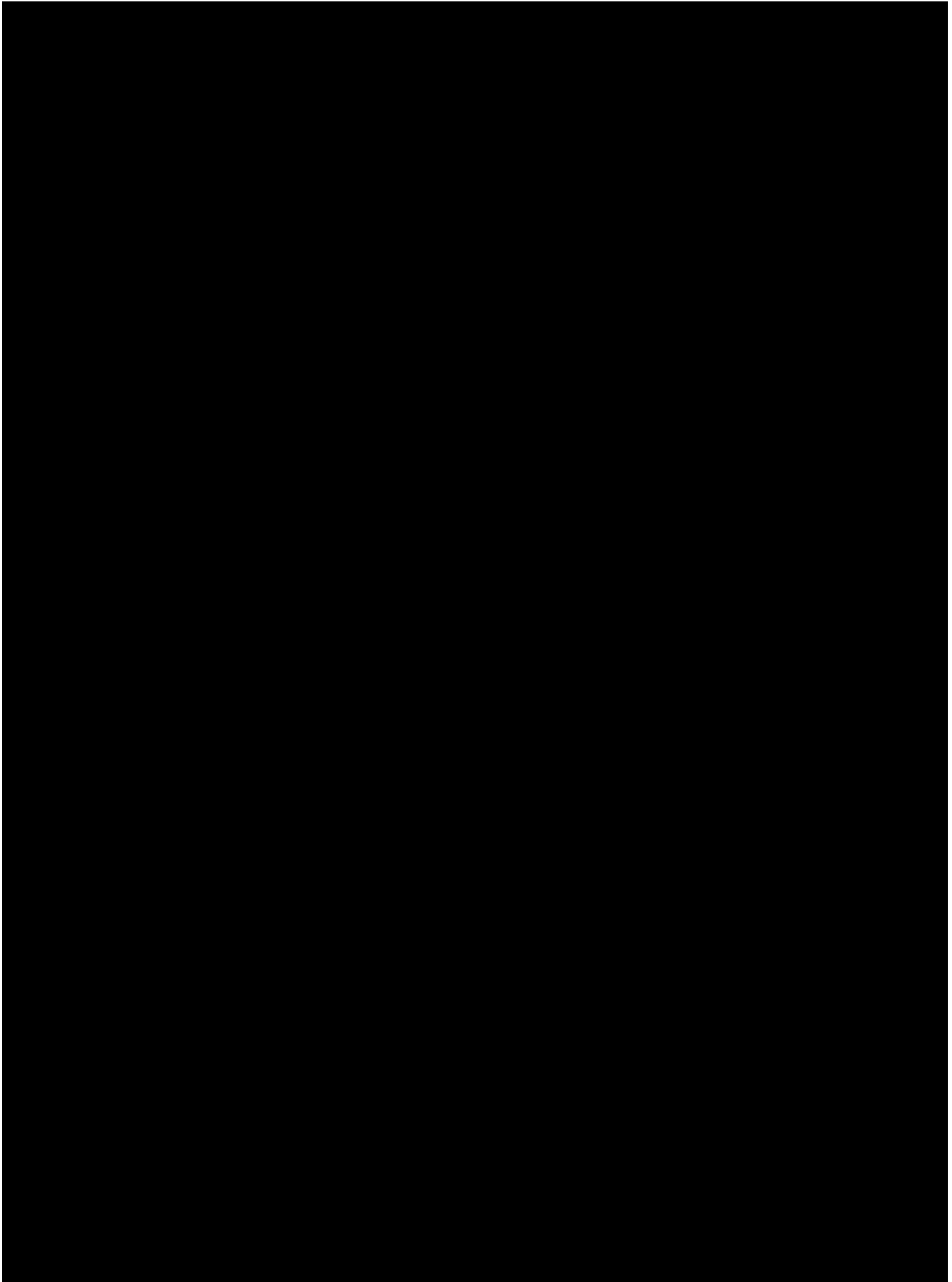
- a. All project management tools needed to deliver the Solution and meet Business and Technical and Management Specifications.
 - b. Approach and tasks for monitoring and controlling the project's schedule, scope, budget/resource tracking, risks, issues, change and quality. The State prefers use of Agile frameworks.
-

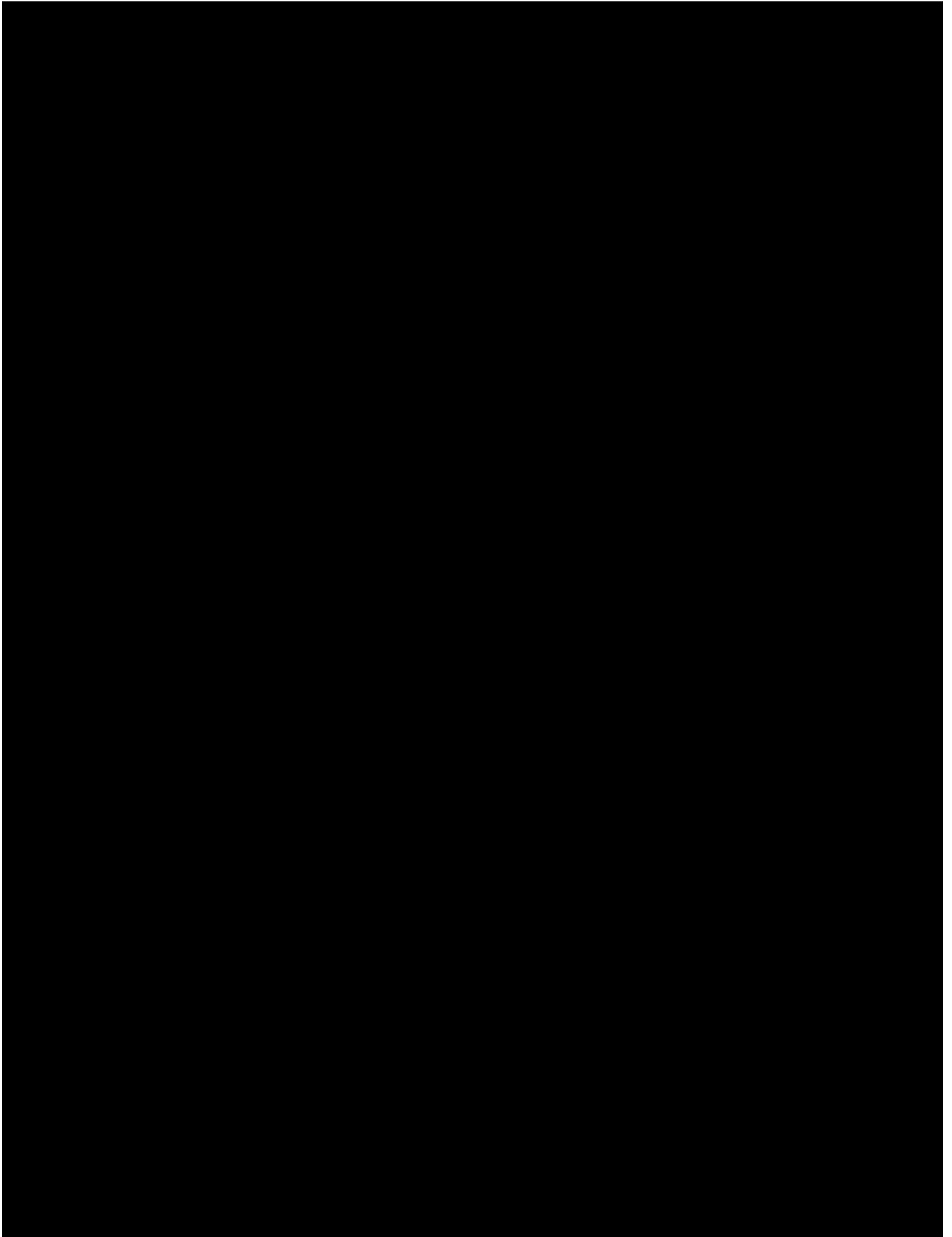


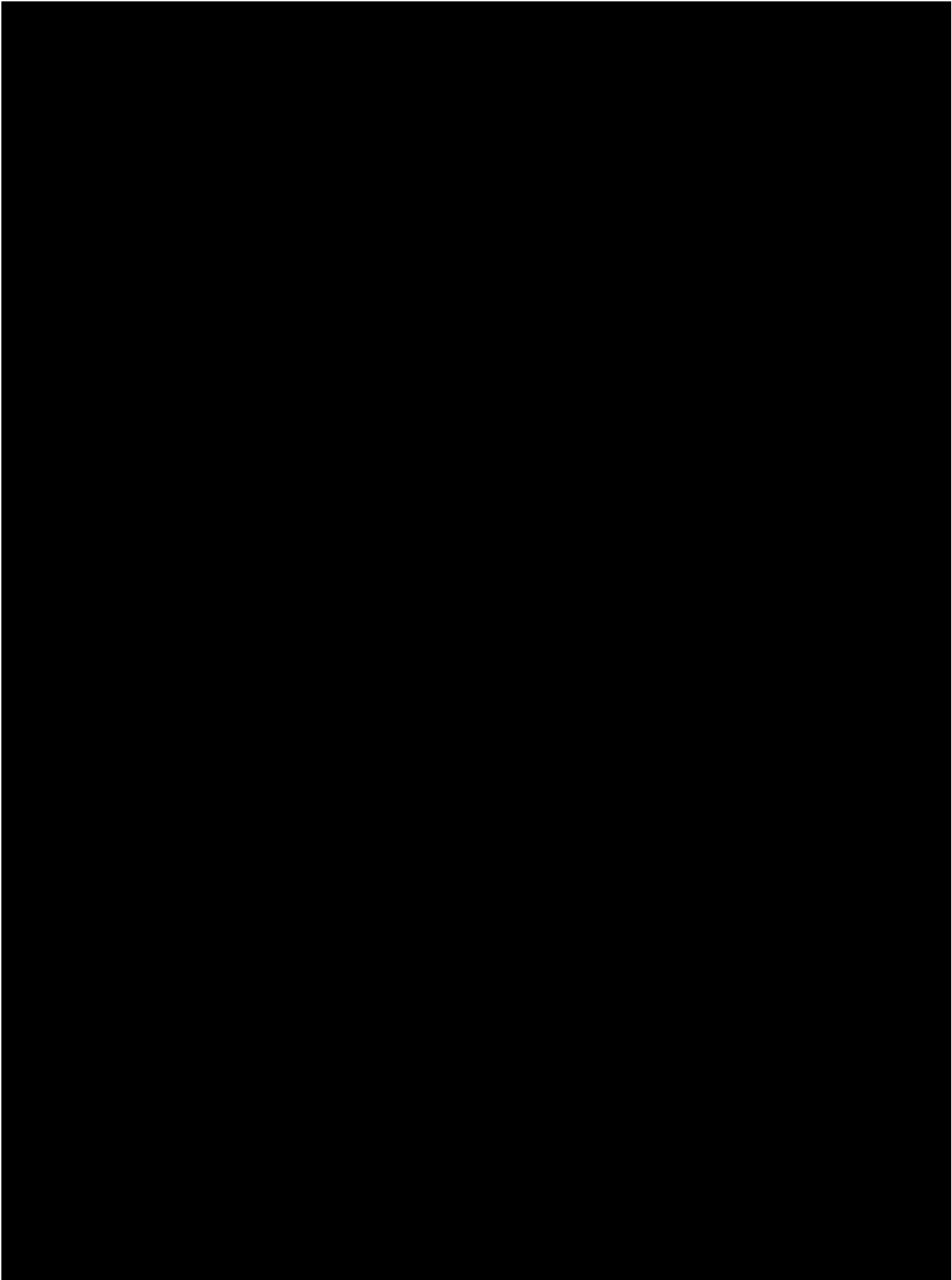


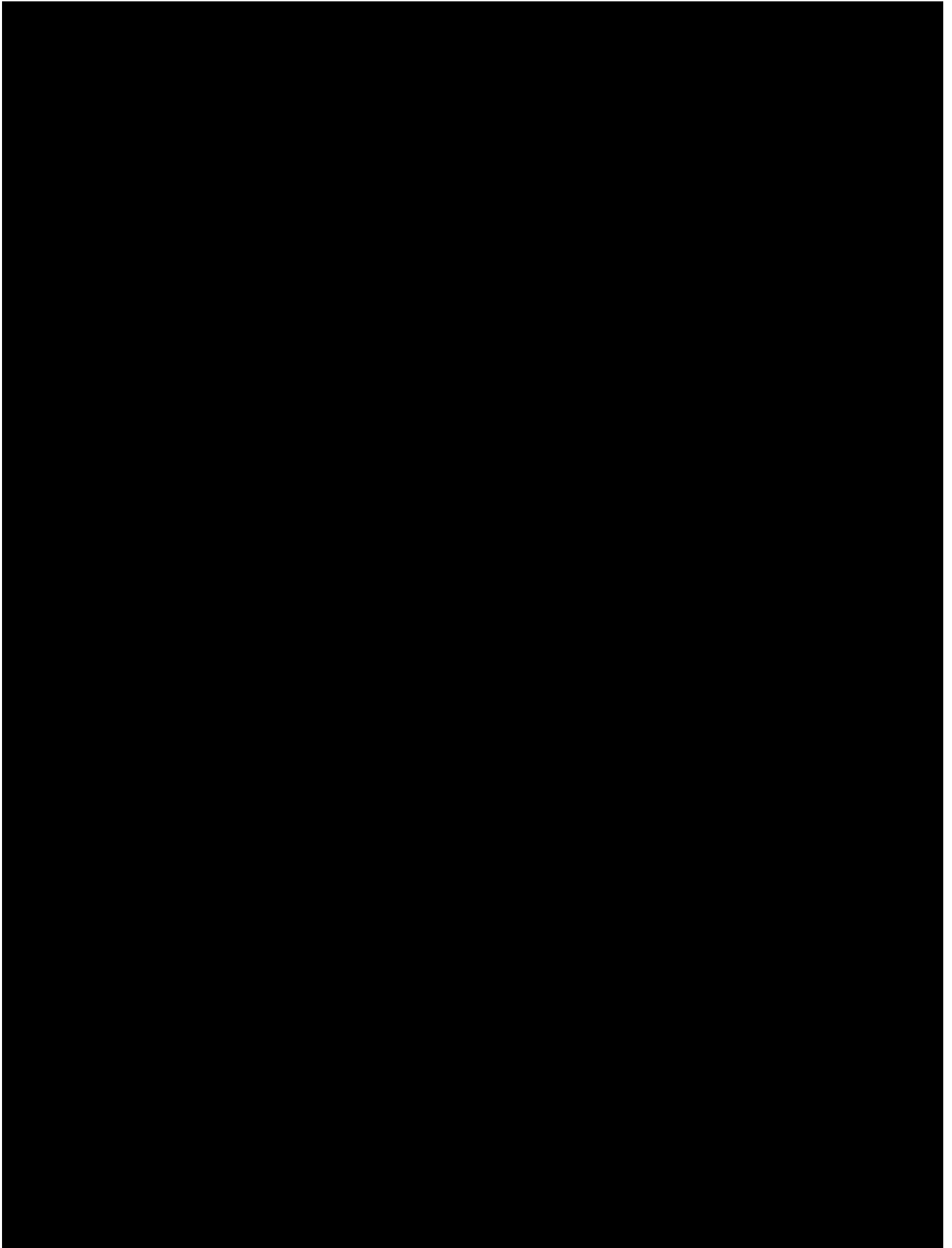












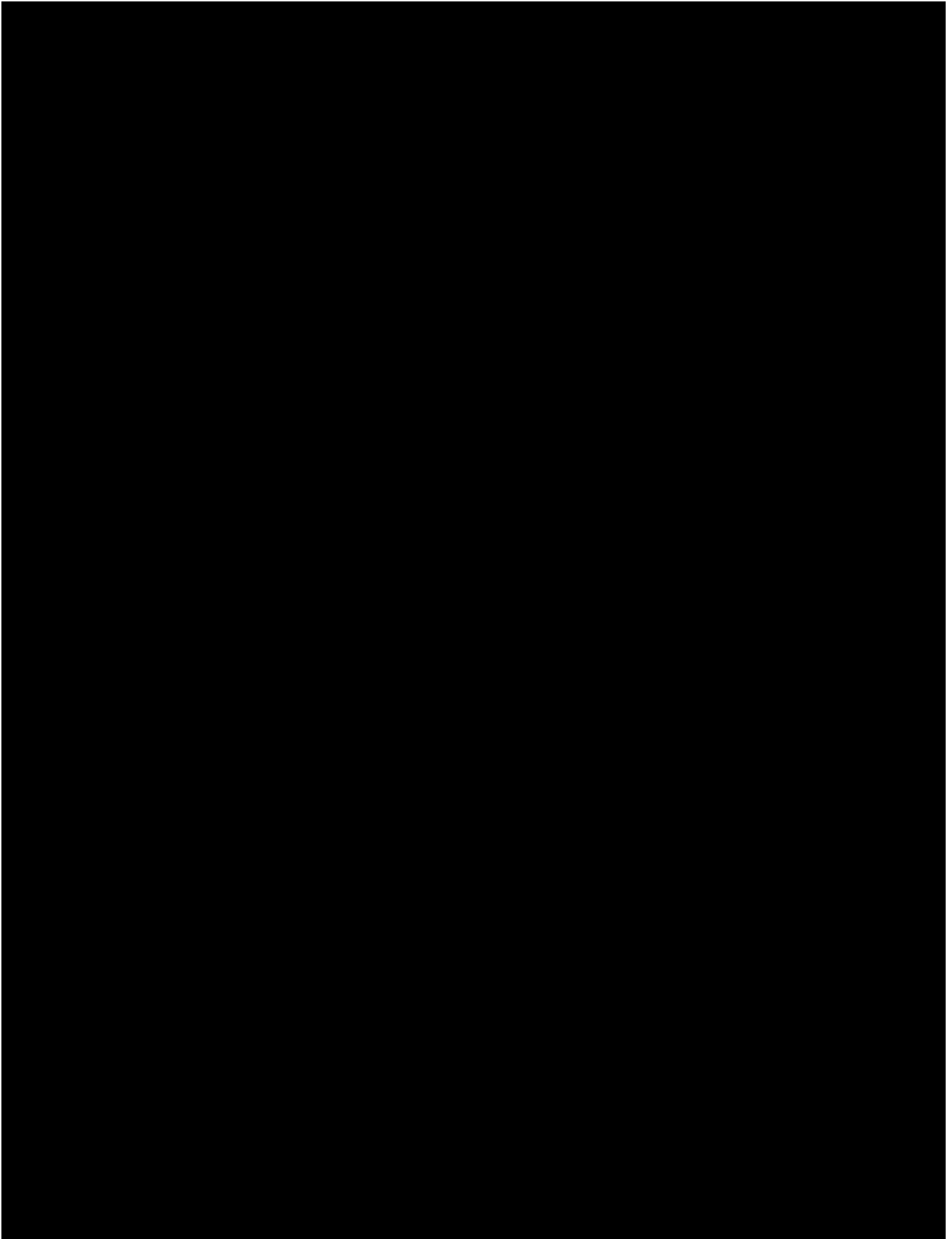
2. Vendor Project and O&M Deliverables

Describe your approach to complete, or assist State personnel in completing, all Project Deliverables according to the Vendor Responsibilities listed in the table provided below in this section during the Project Execution Contract Phase and the O&M Contract Phase. If the Vendor Responsibility is listed as Contributor for a Project Management Deliverable, then the State is the Owner and is responsible for the completion of the Project Management Deliverable, with Vendor assistance. If the Vendor is listed as the Owner, then the Vendor is responsible for completion of the Project Management Deliverable, with State assistance (i.e., State is the Contributor).

Reference Attachment J: Minimum Content for Project and O&M Deliverables for description of and provision requirements for Project Management Deliverables. (The requirements set forth in Attachment J: Minimum Content for Project and O&M Deliverables apply to the deliverables during the contract term.)

Mapping of Deliverables to Requested RFP Deliverables

The image consists of a single, uniform black rectangle covering the entire area. There are no discernible features, text, or patterns.

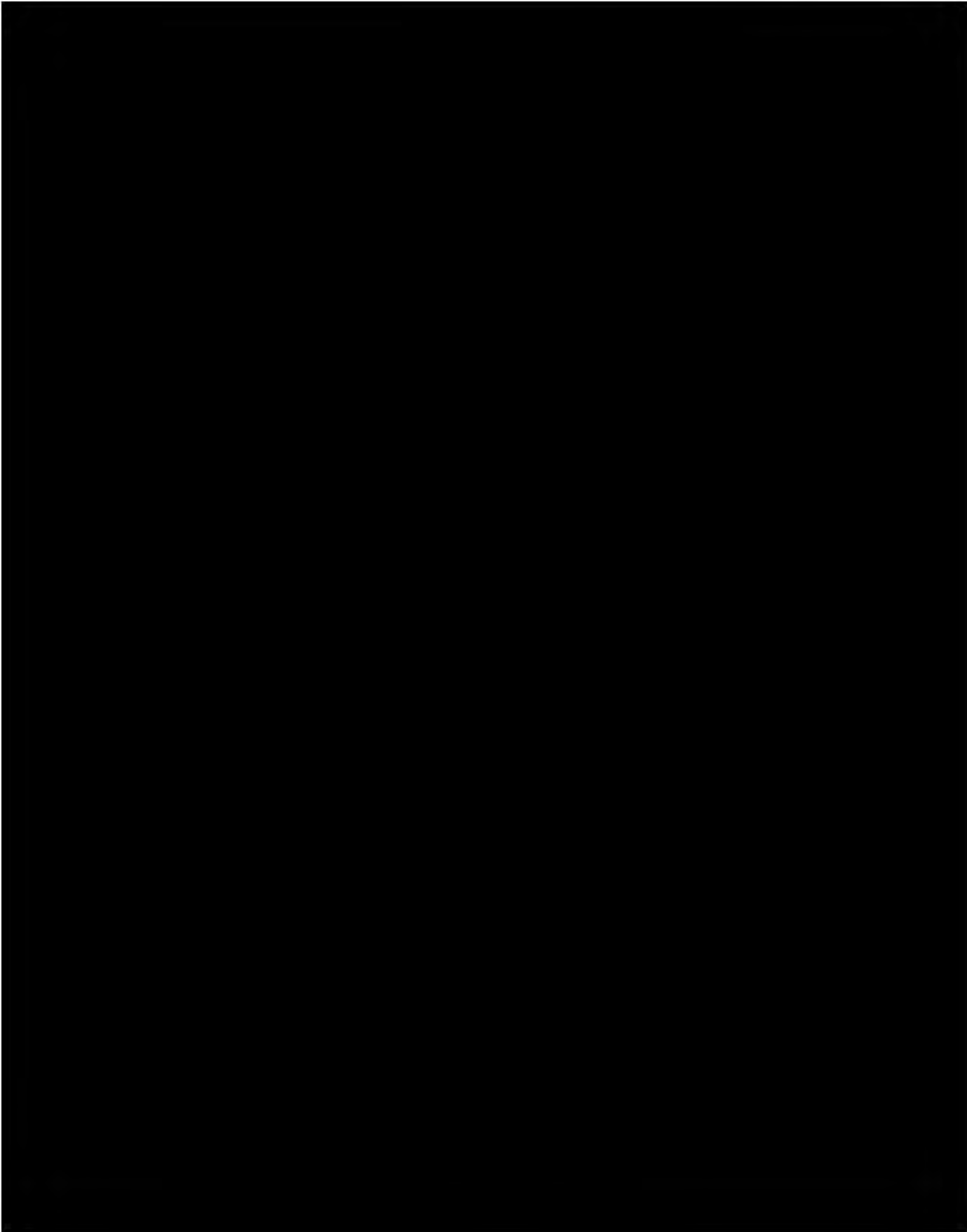


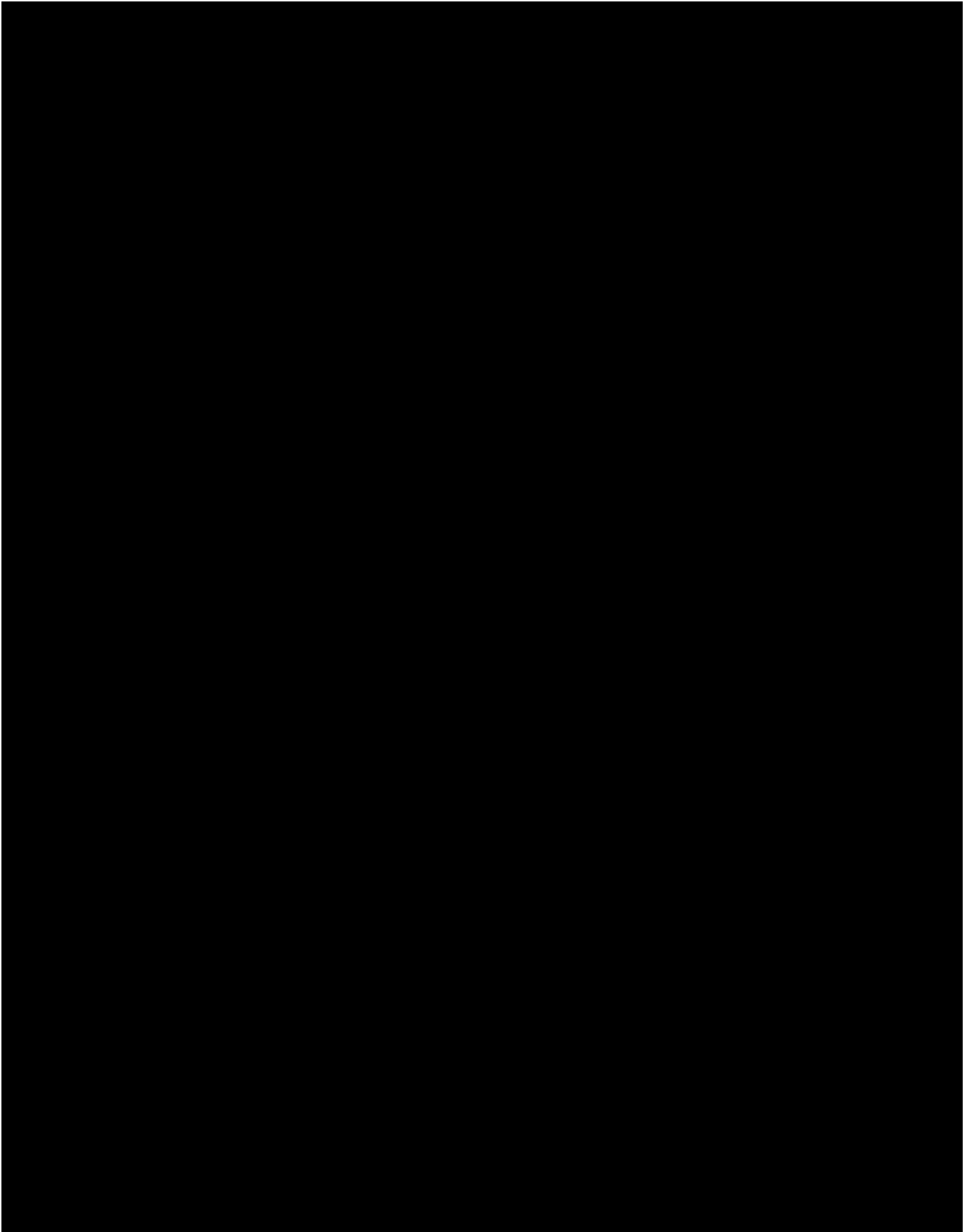
3. Vendor Project Staffing

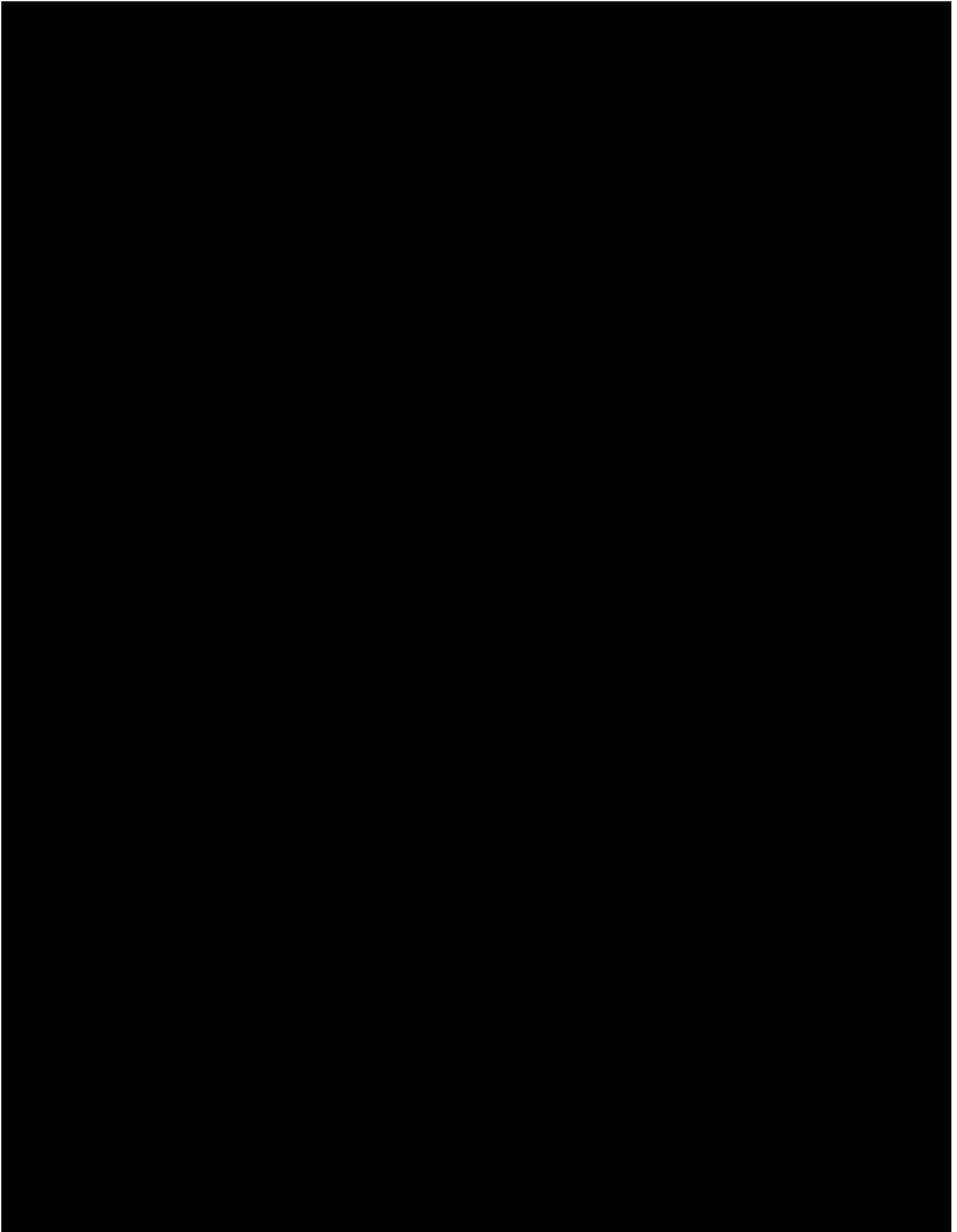
Vendors are to include a draft project schedule in their response that includes and describes all planning activities, development activities, pilot, and deployment as well as the Project Management Deliverables listed in Section 3.5.2.2 above. For each Project and O&M Deliverable in the table above, Vendor shall identify Vendor and/or State personnel required to complete the task in the project schedule.

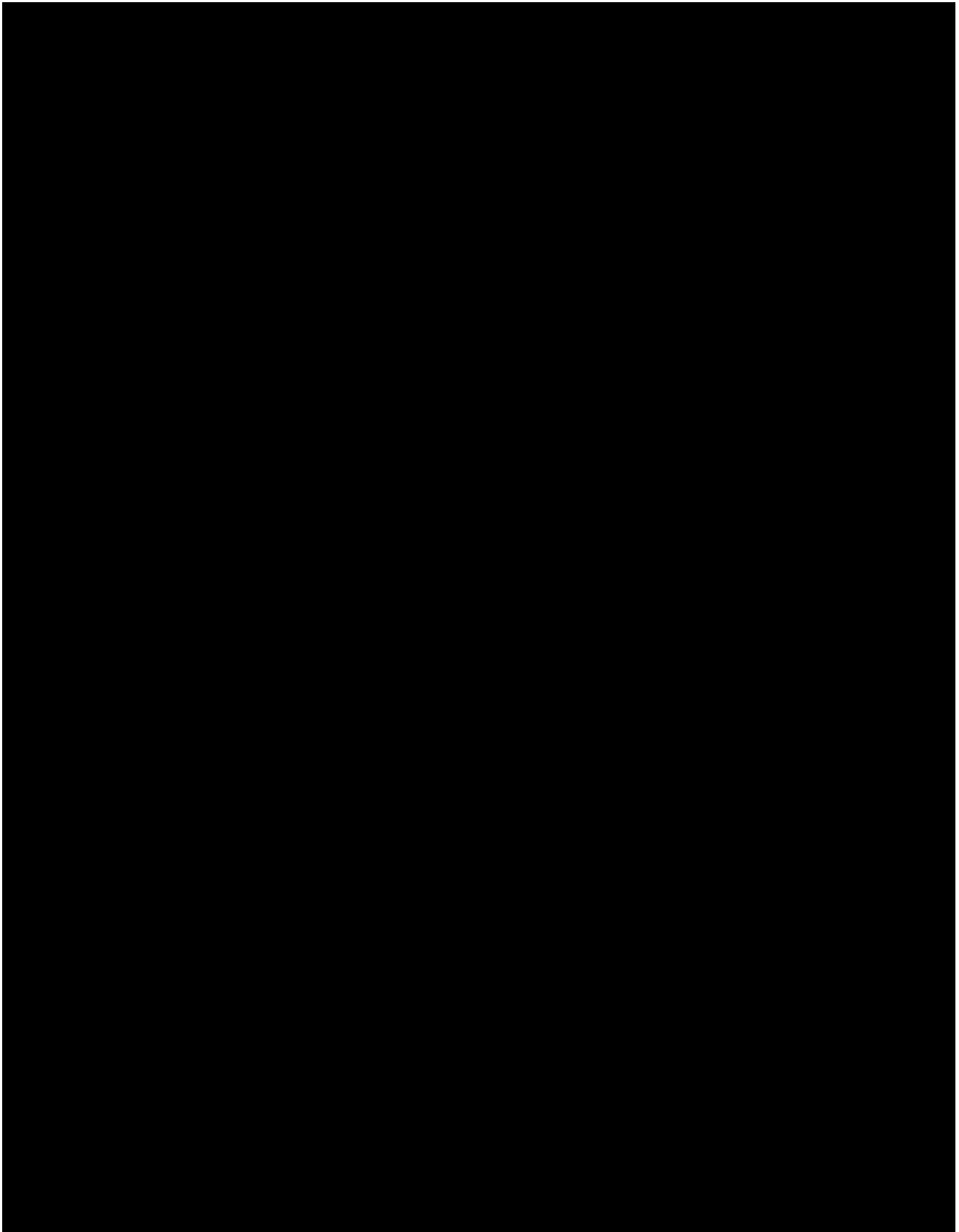
At Accenture, our commitment to DCDEE is driven by an unwavering focus on results. Every child and family in North Carolina deserve unparalleled childcare services. With this in mind, we've assembled a team with extensive experience in child services, regulatory management offerings, and state-of-the-art Salesforce technological solutions. These tools empower us to use analytics to gain insights, minimize risk, and foster improved outcomes more swiftly.

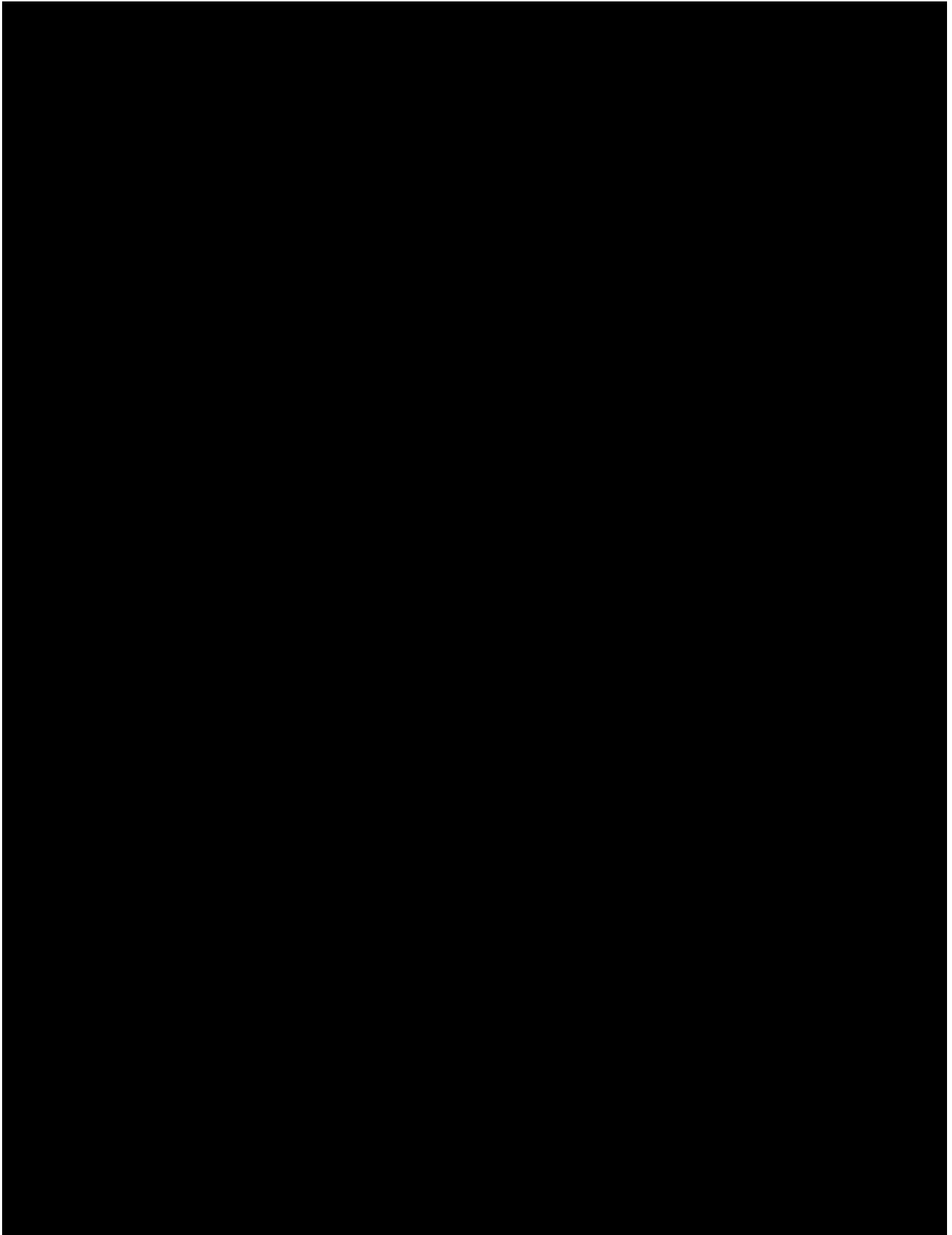
Choosing the right collaborators is pivotal for success in North Carolina. Our promise is to work closely with you, ensuring NC-PROCEED's delivery on time and on budget. Our team comprises a diverse mix of industry professionals and technology experts, all equipped with specialized skills. Their expertise spans areas such as Social Services, Regulatory, Childcare and K12 Program Management, User-Centered Design, Data Analytics, Child Services Systems Implementation, Salesforce and Boomi.

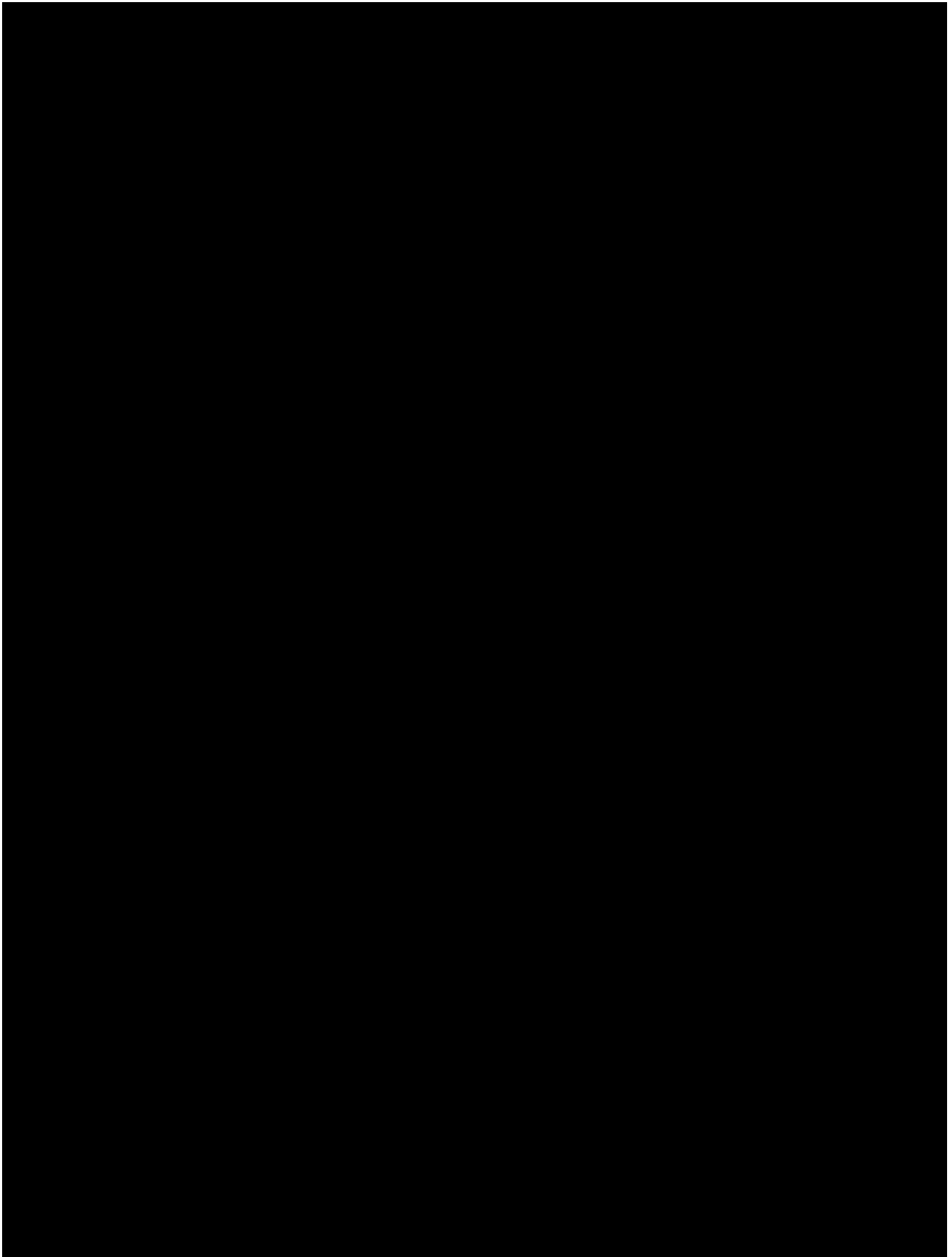


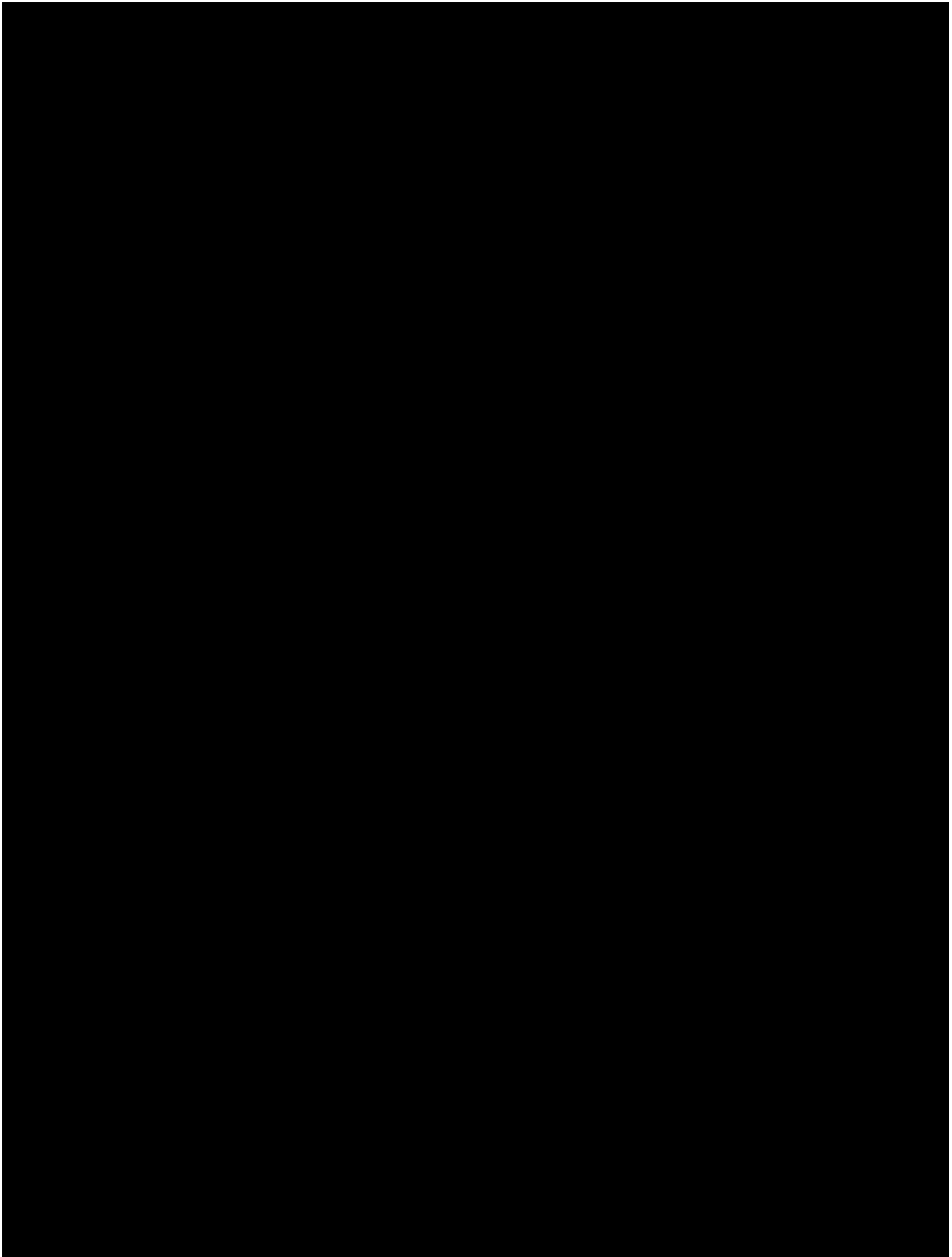


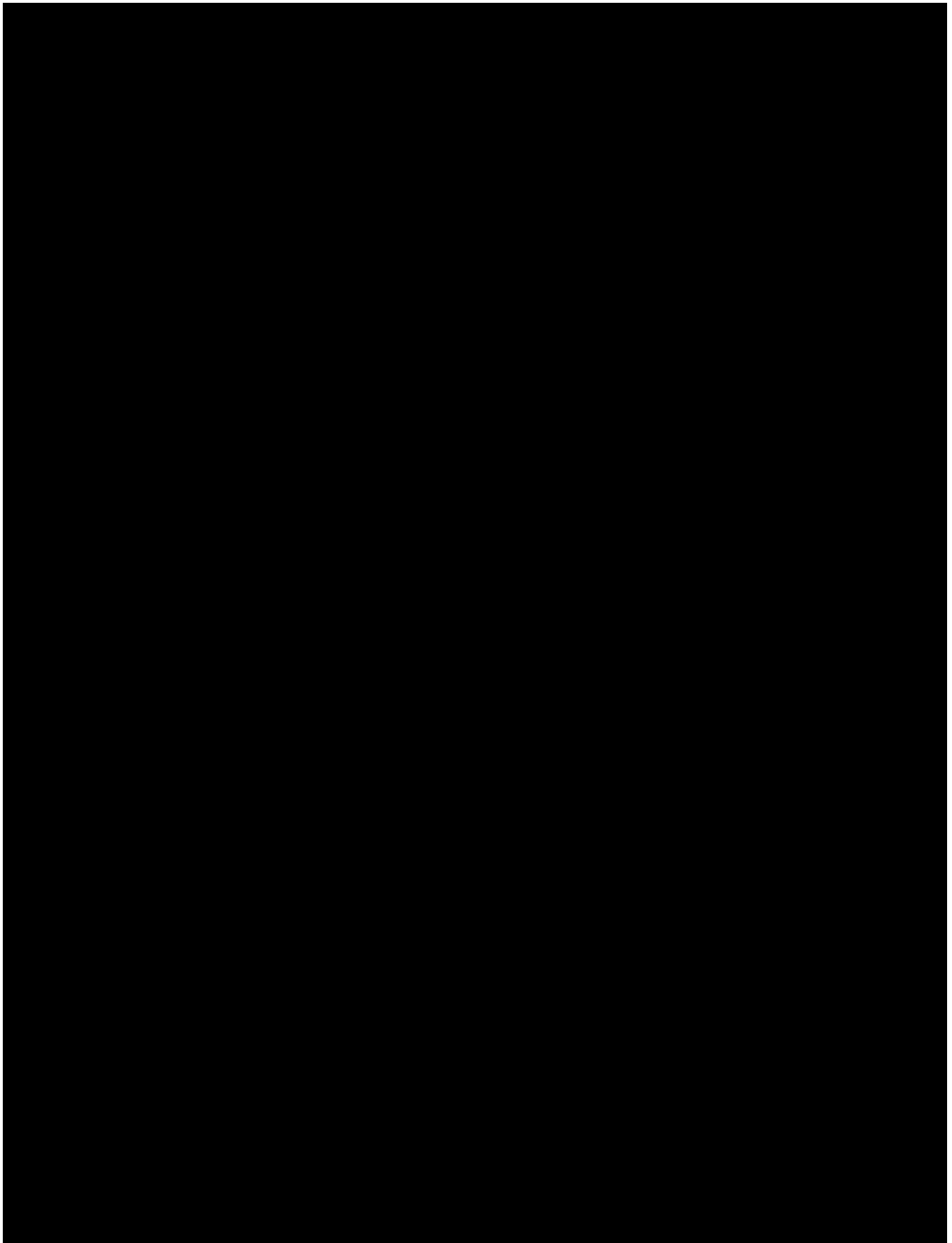


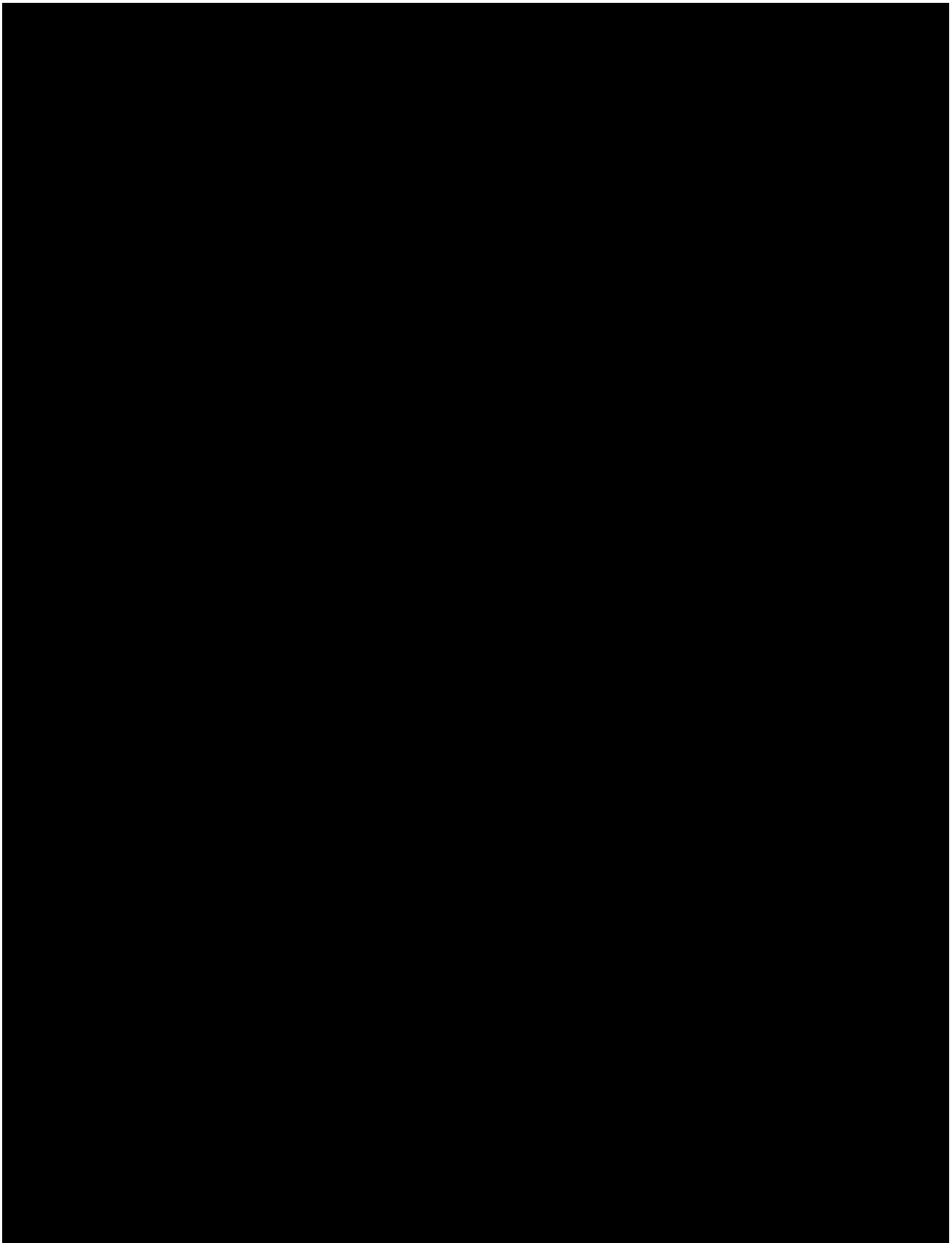


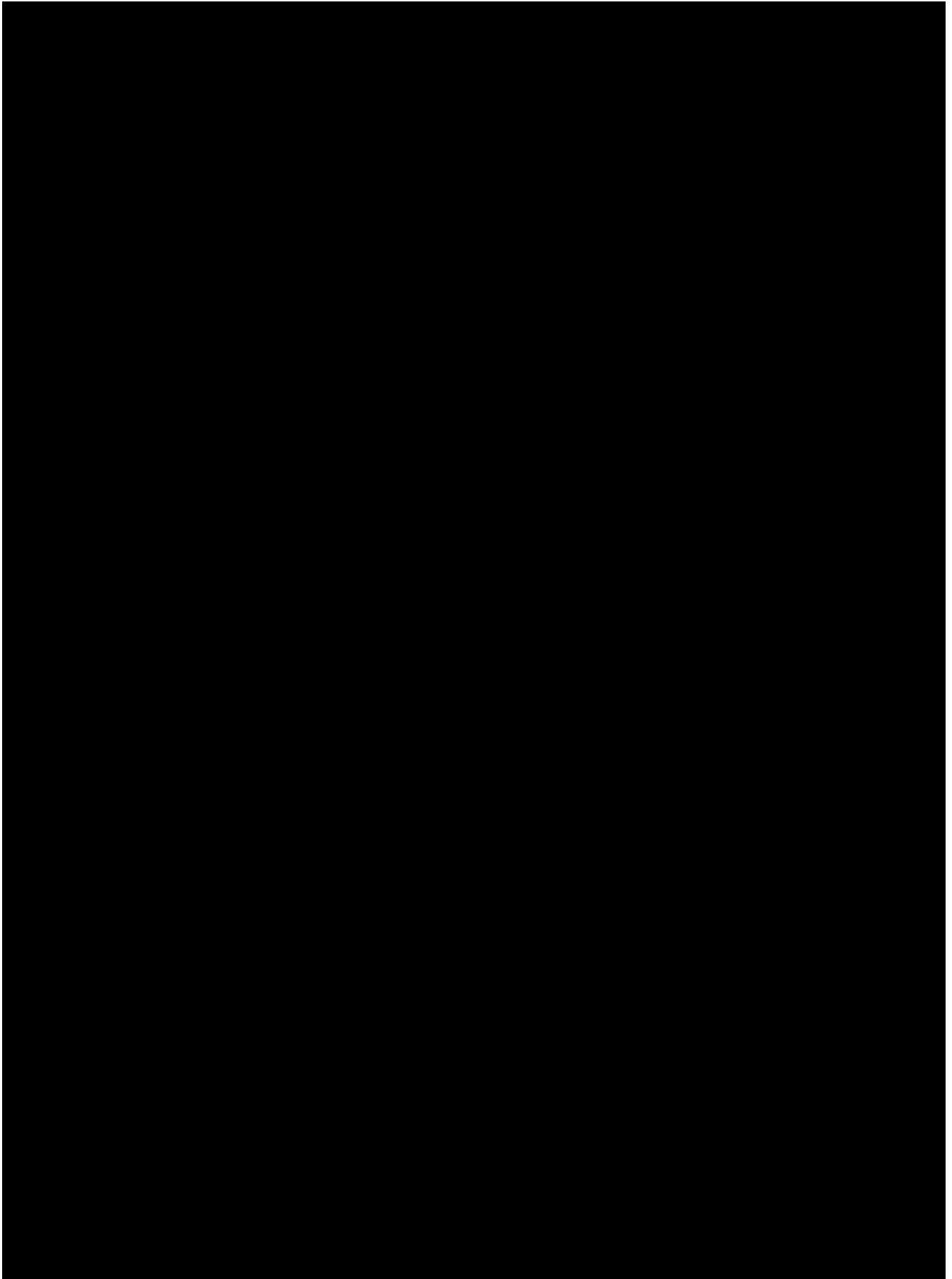


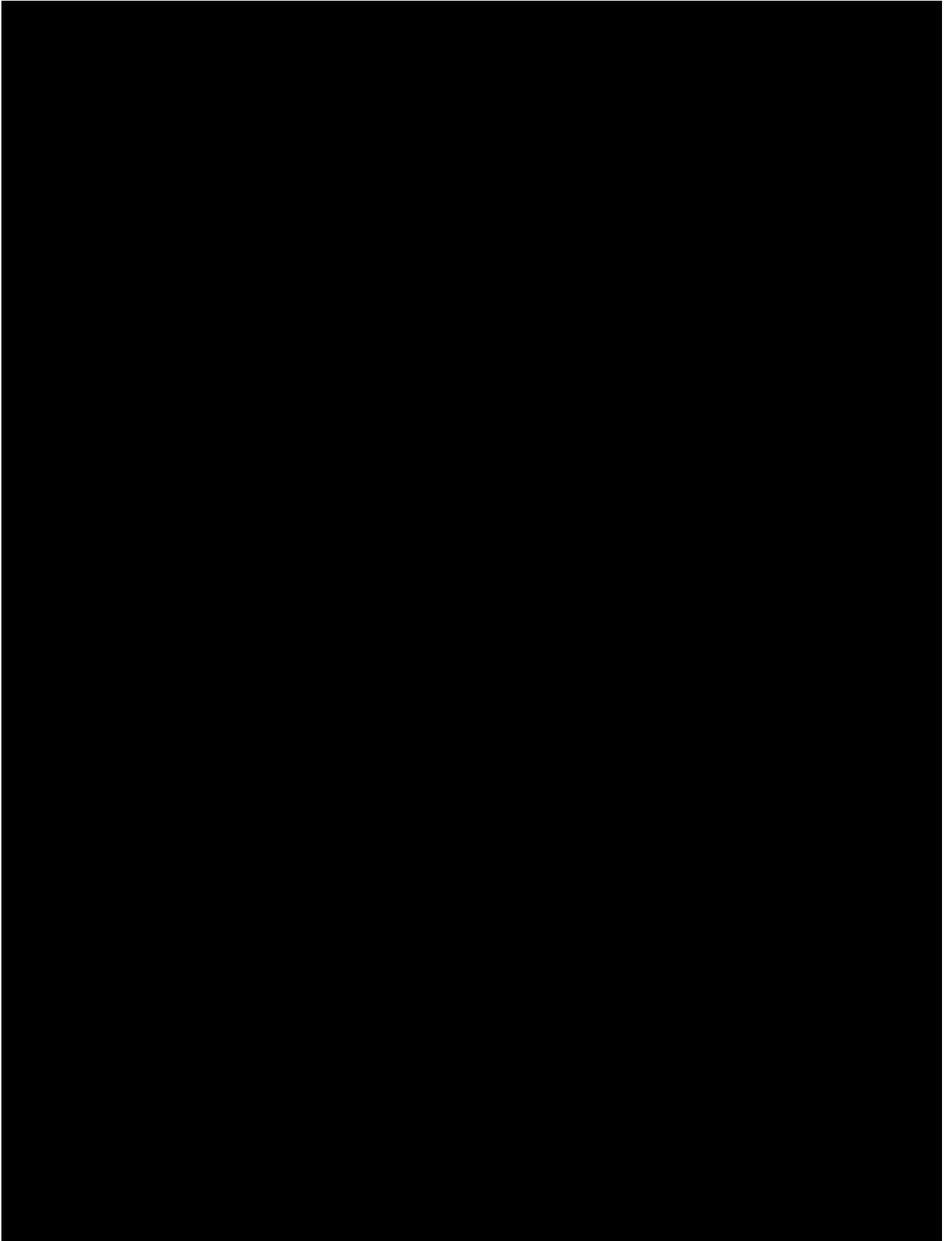


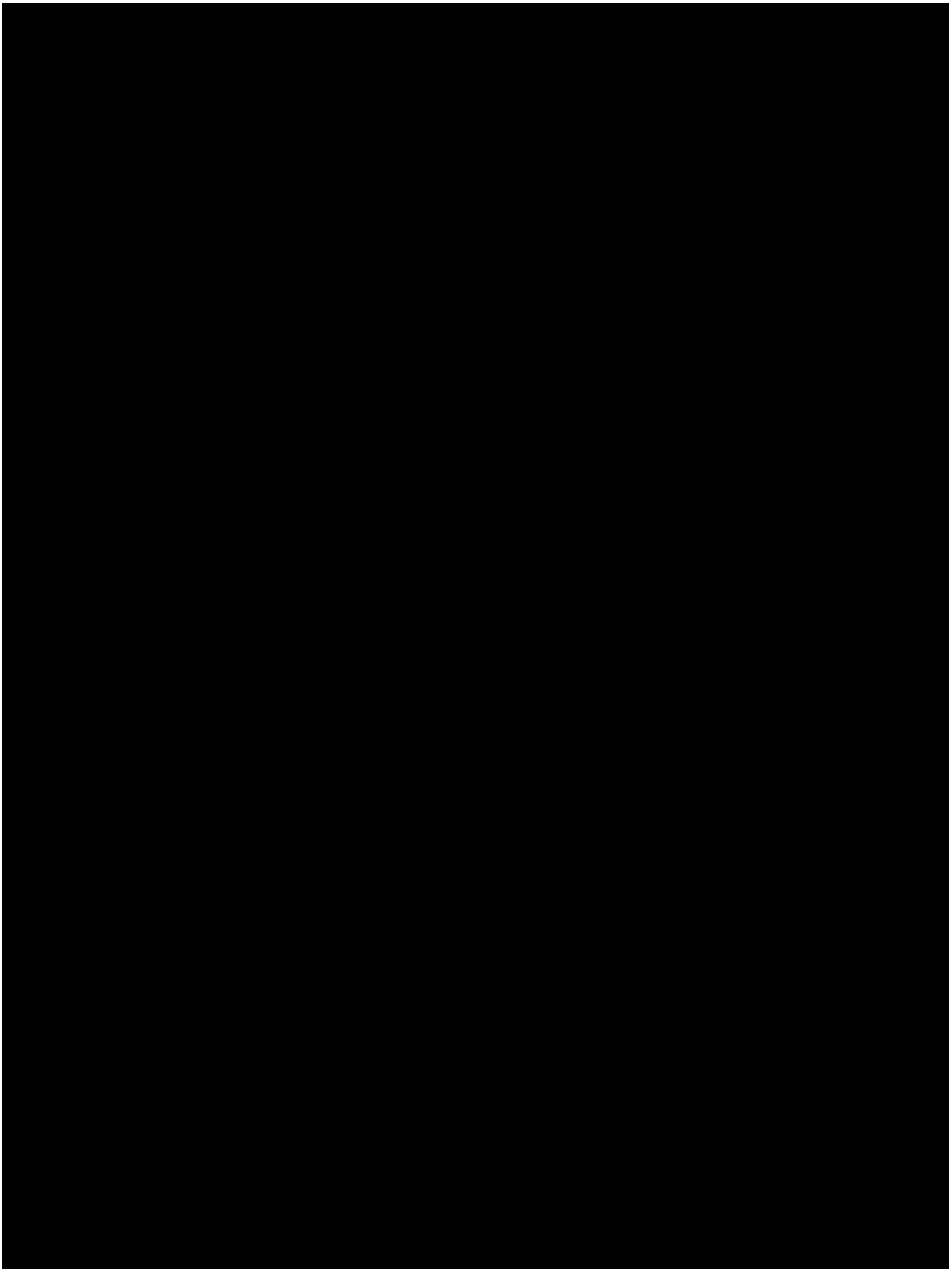


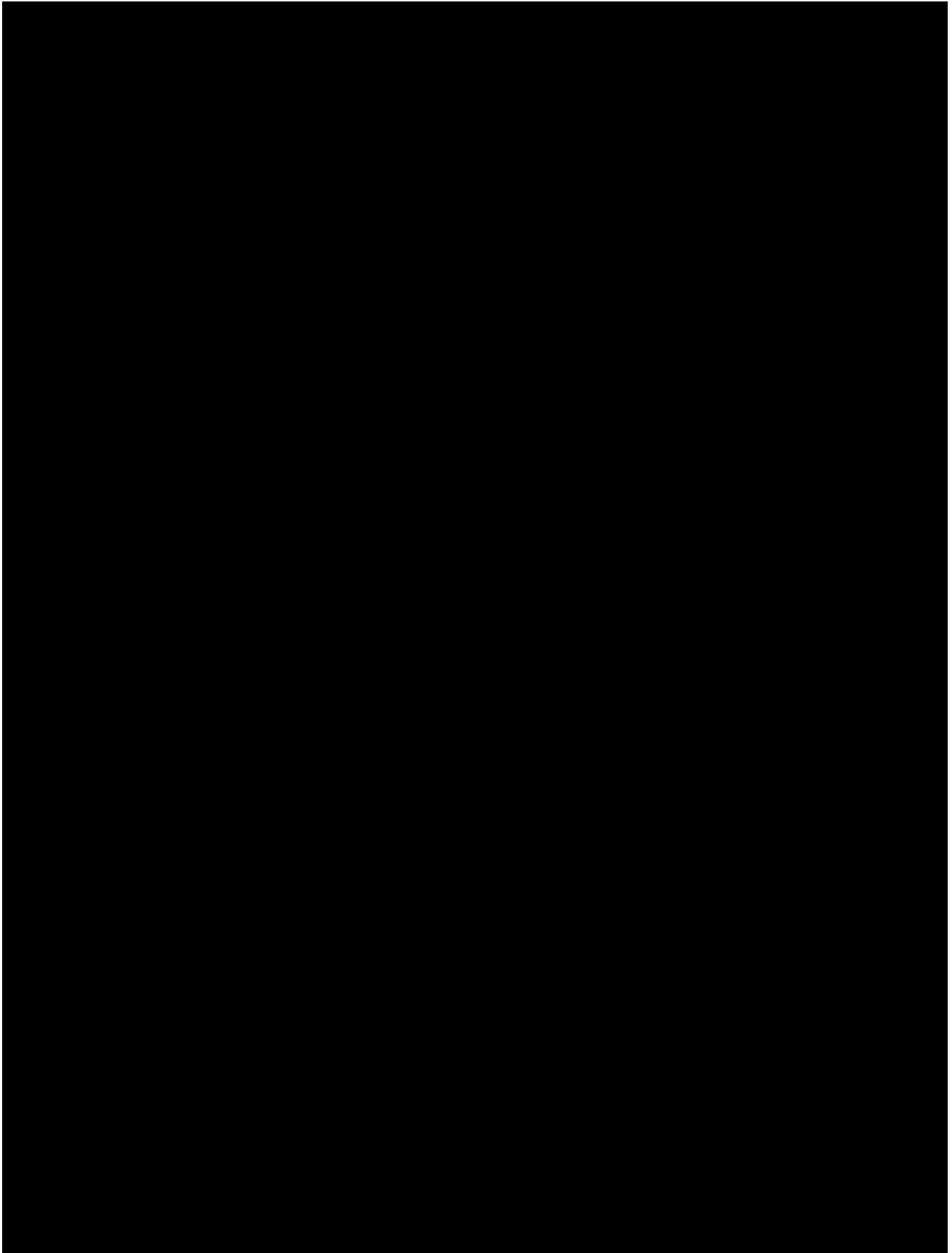


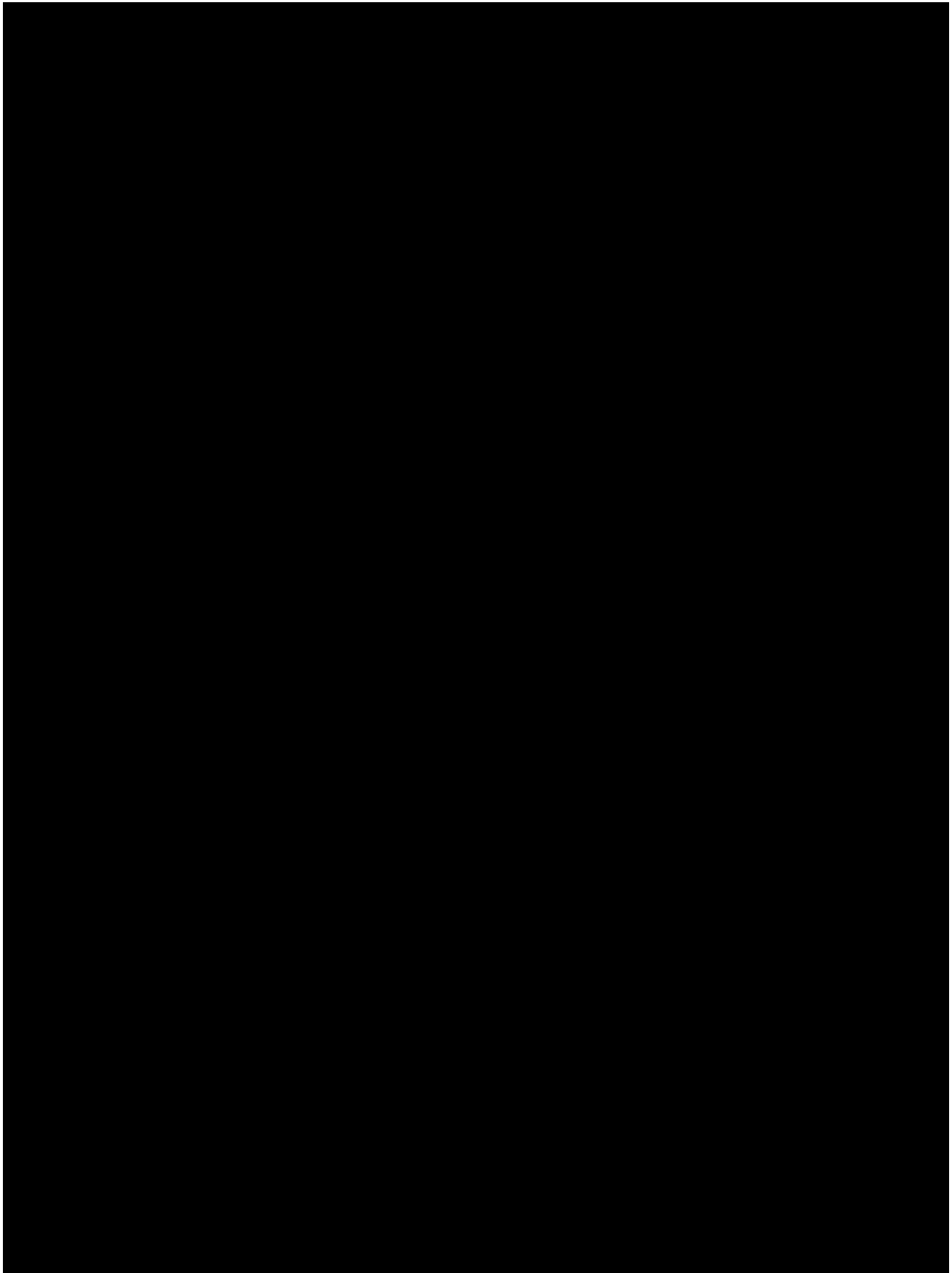


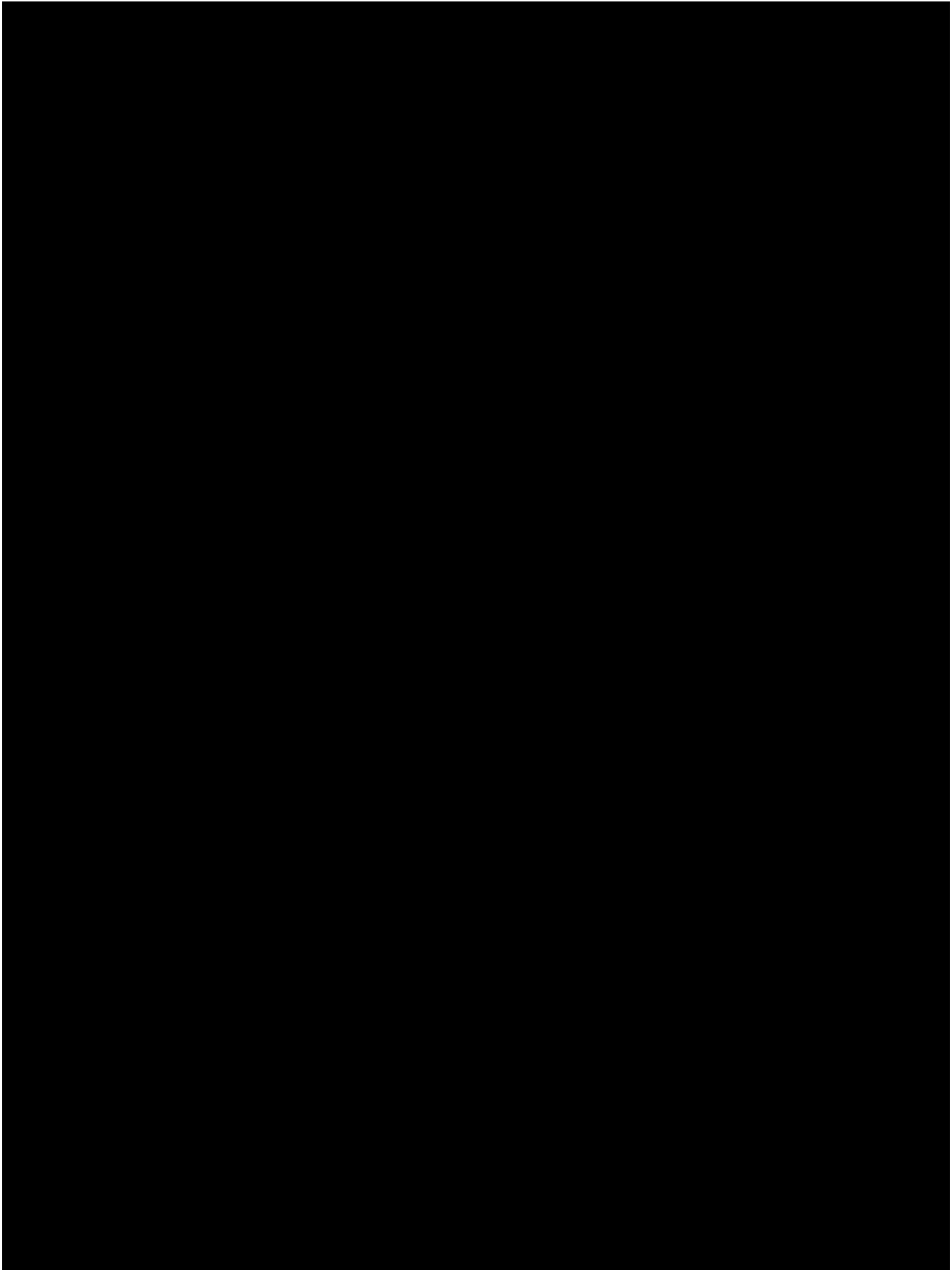


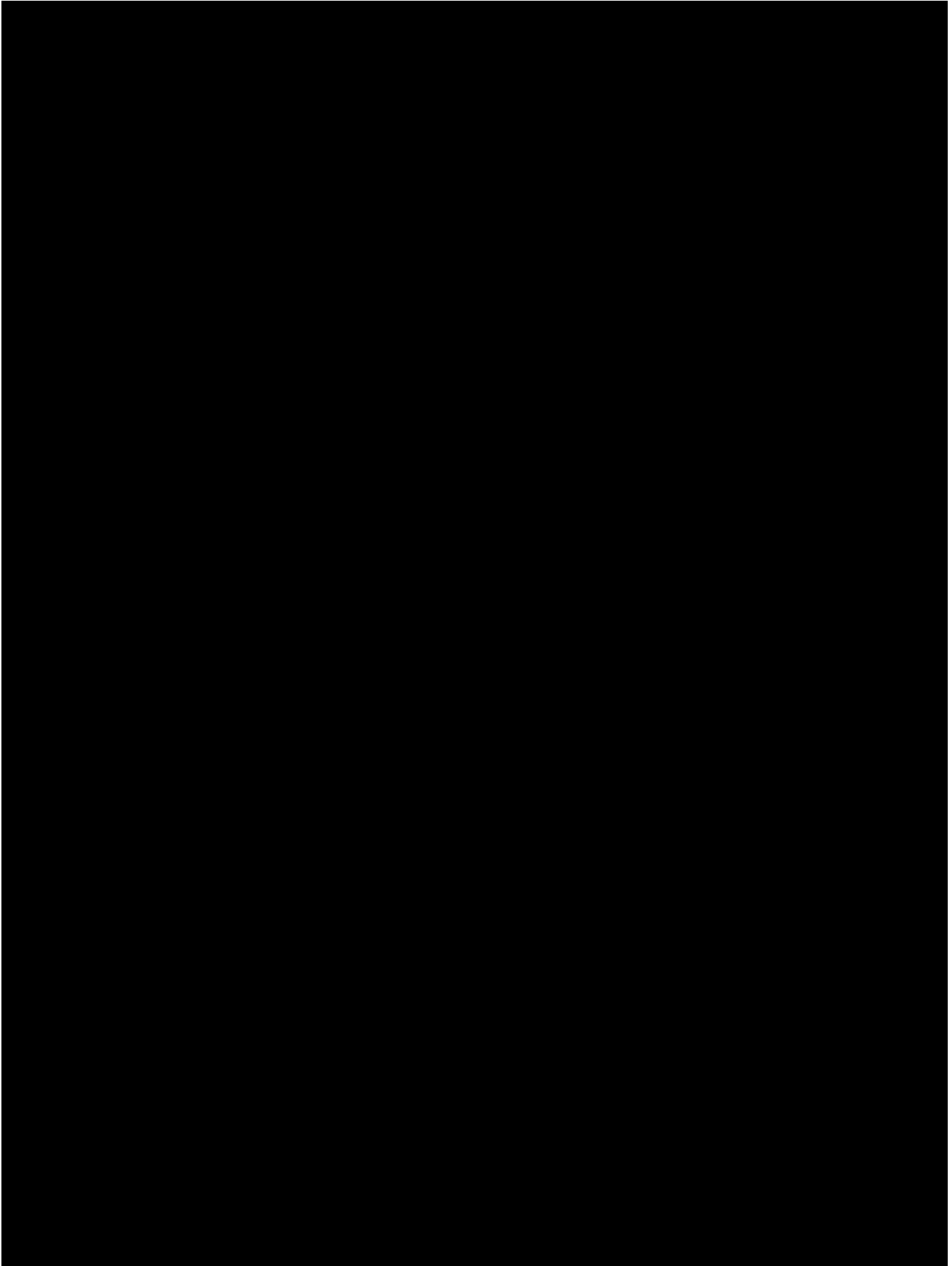


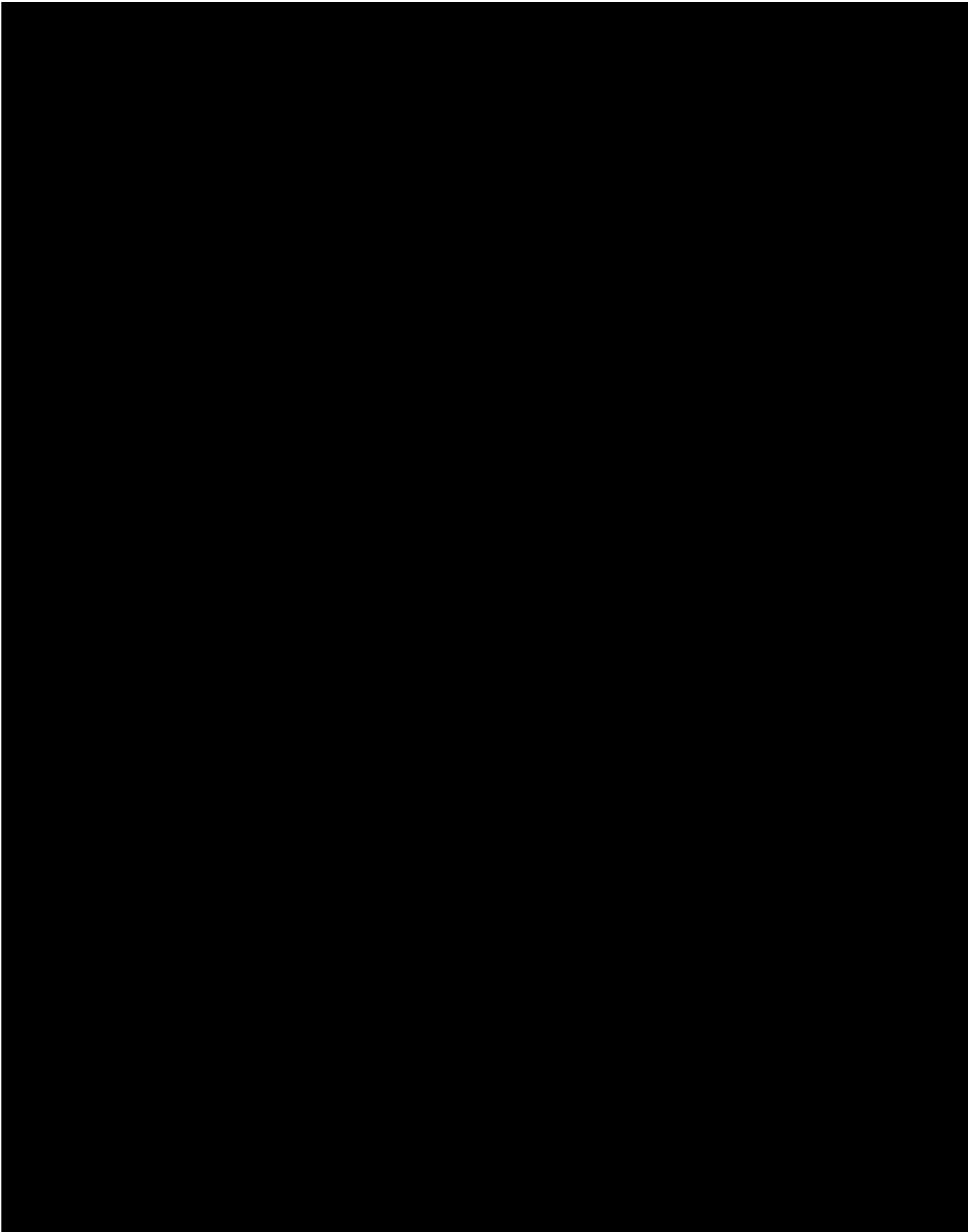


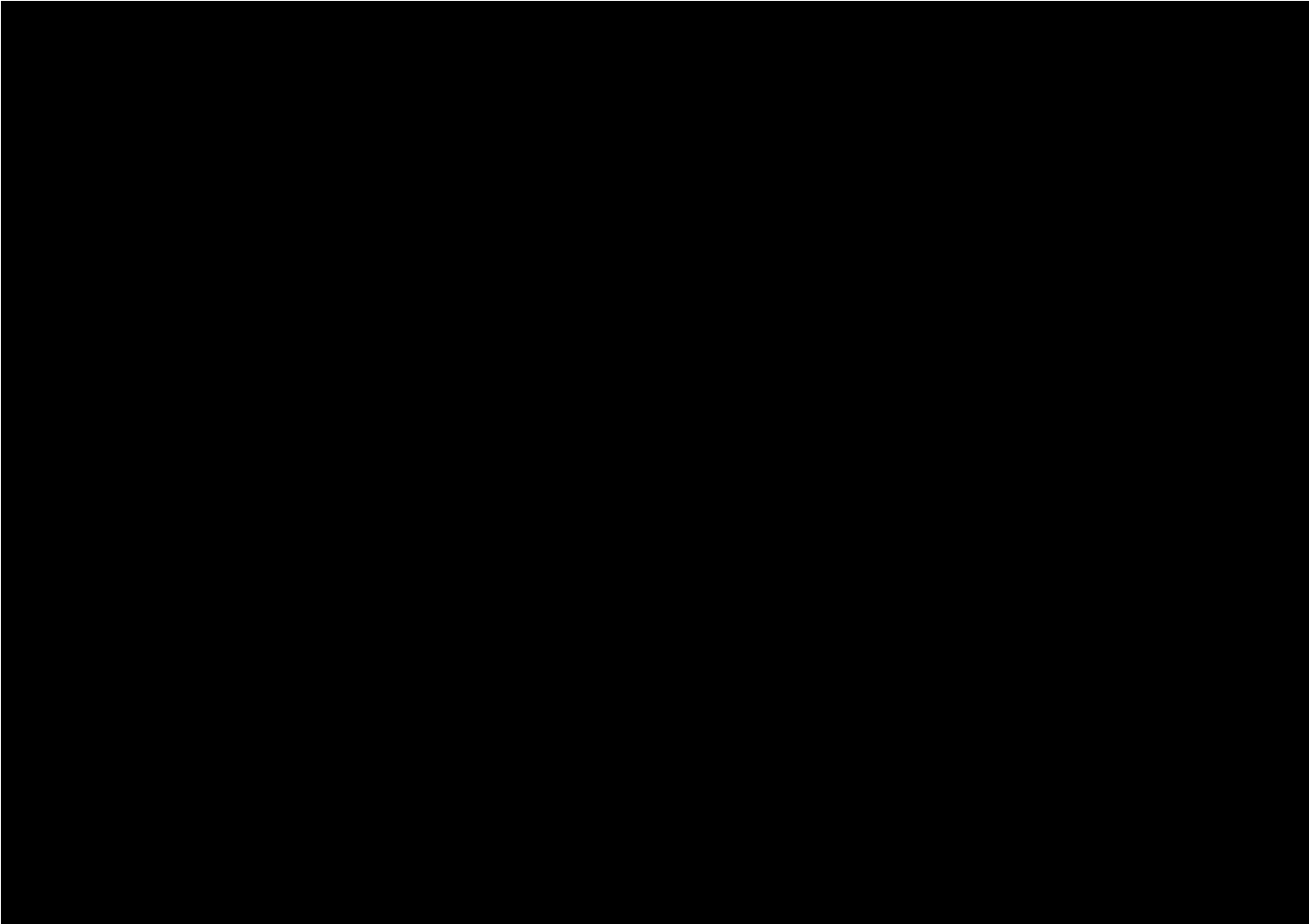








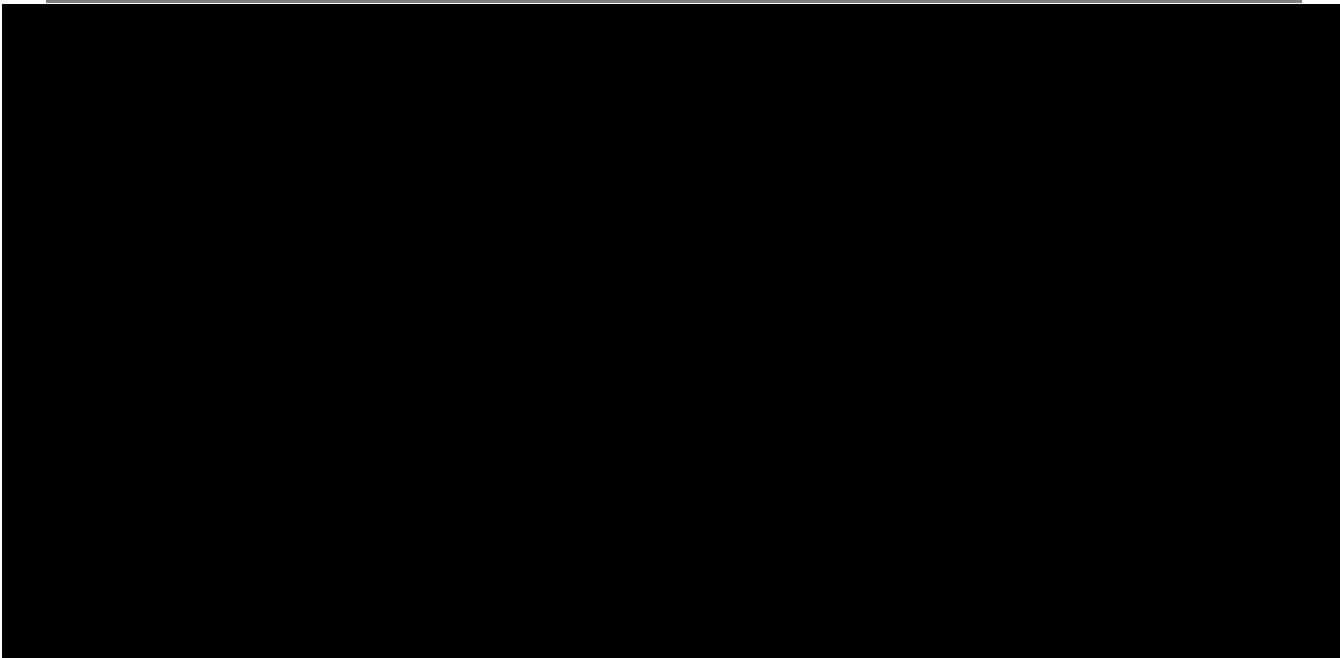


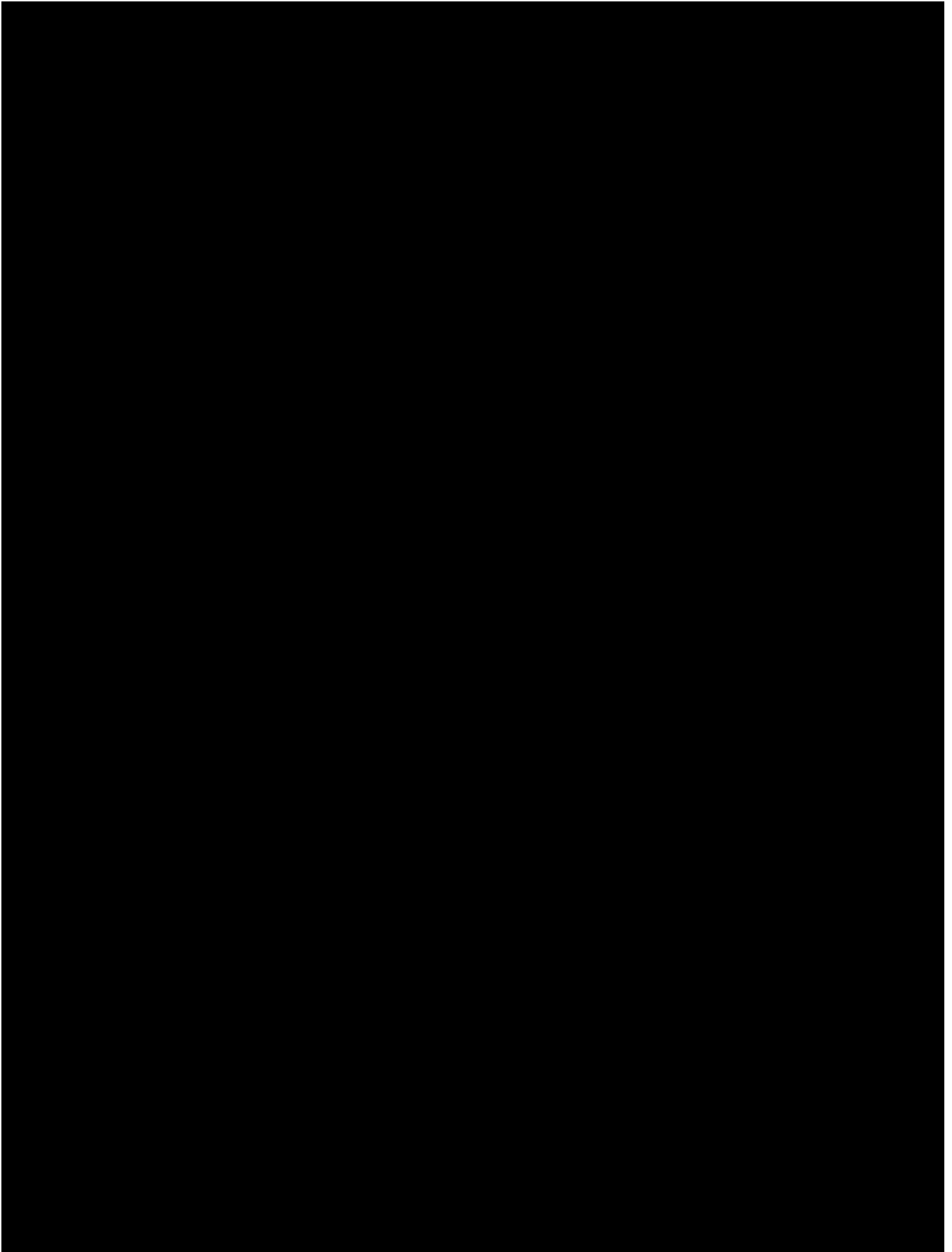


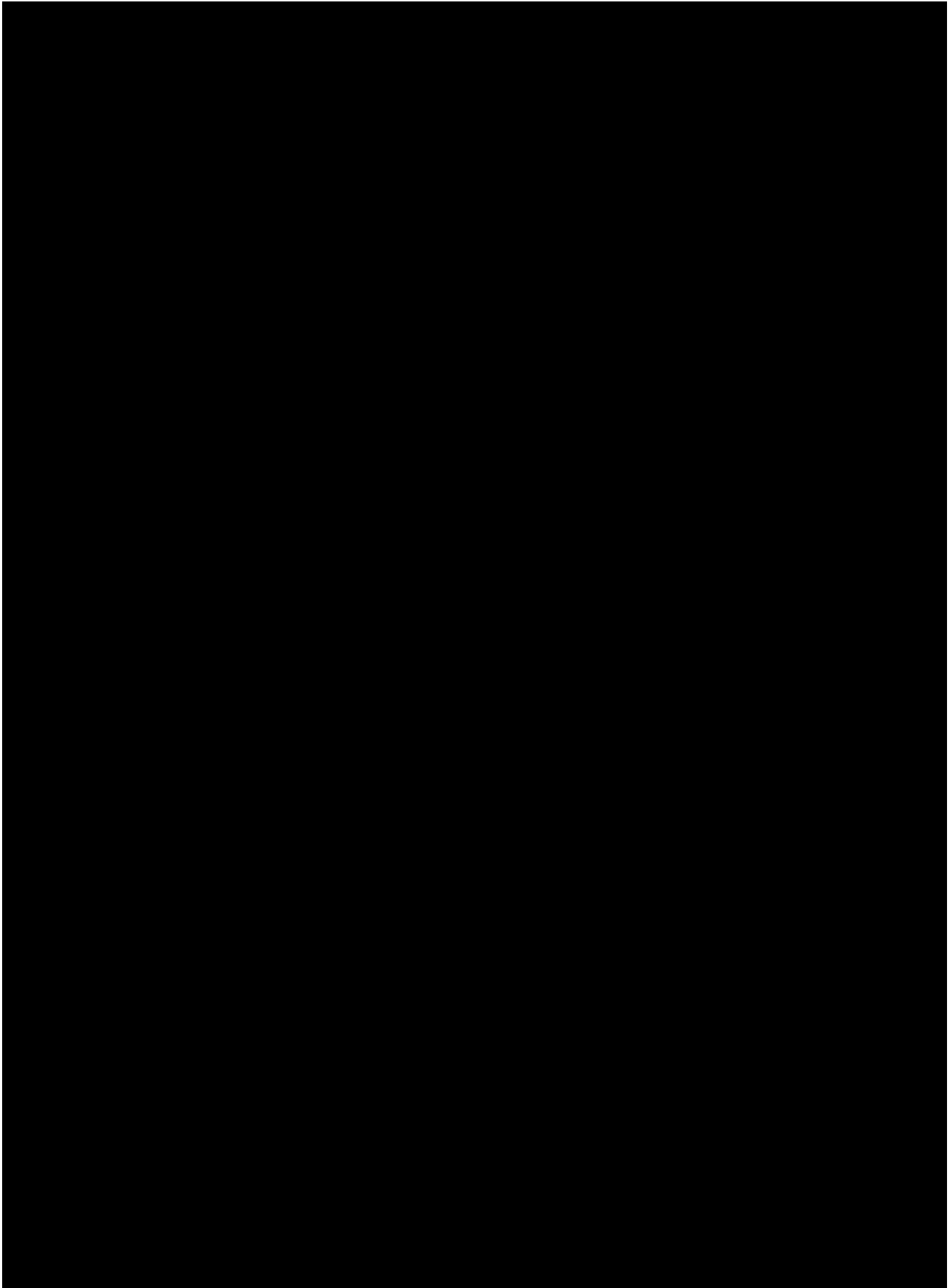
4. Releases/Production Deployment and Support

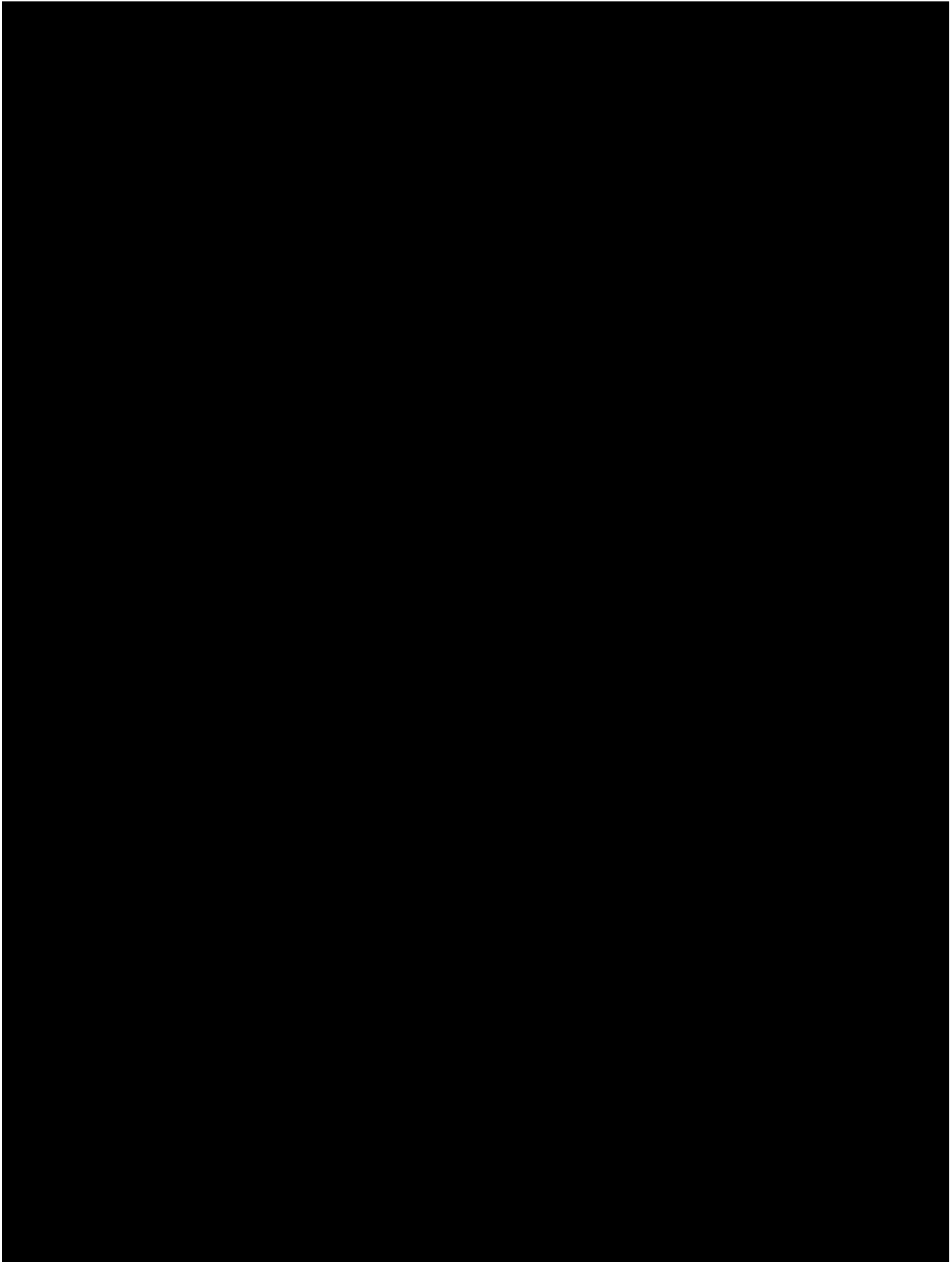
Describe your approach to deploying the developed Solution for production use, including the following items below in your RFP response:

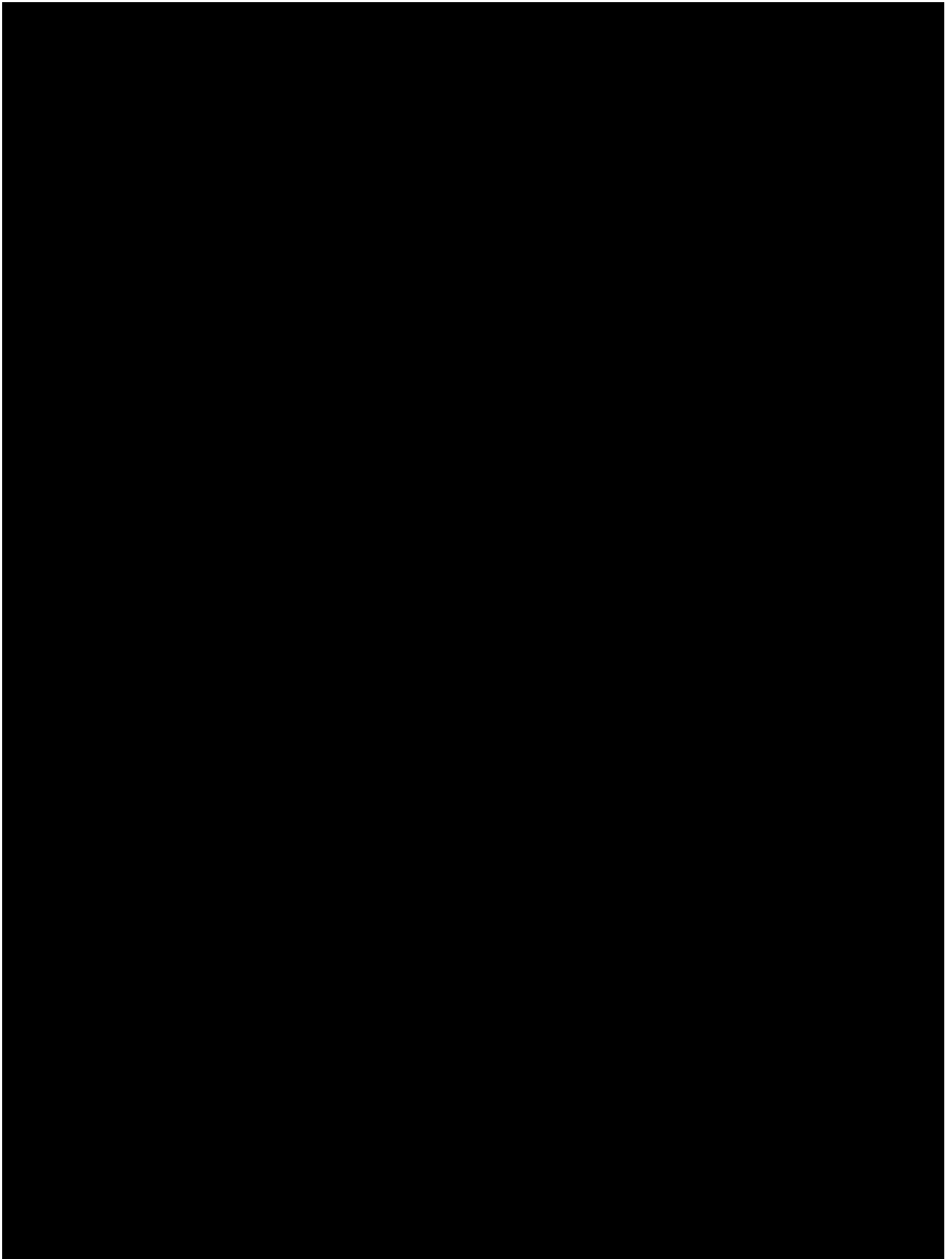
- a. The strategy for deploying the Solution for production use, including the number of Releases proposed;
- b. Deployment planning and preparation, including site visits, site readiness verification, end user device upgrades;

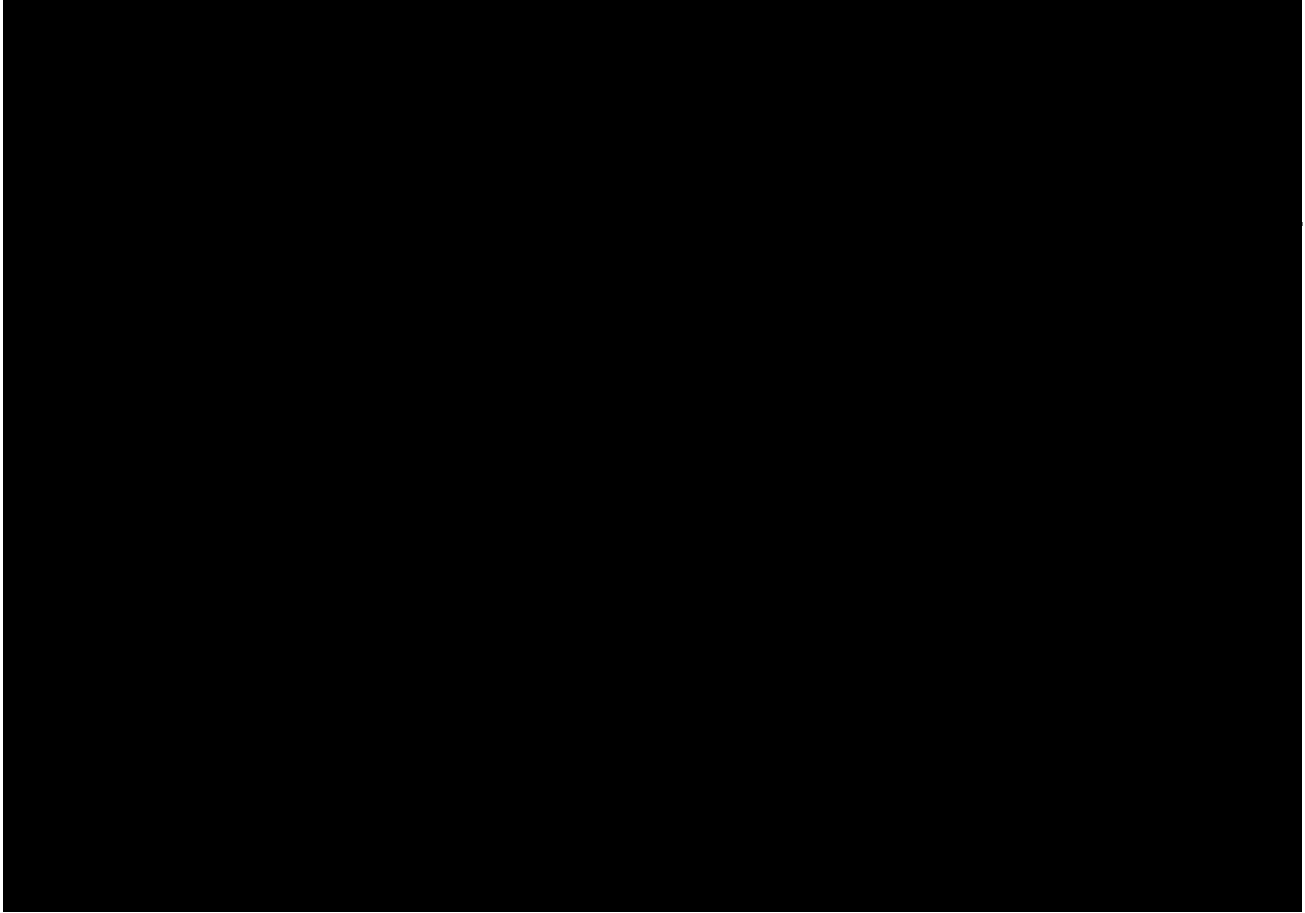






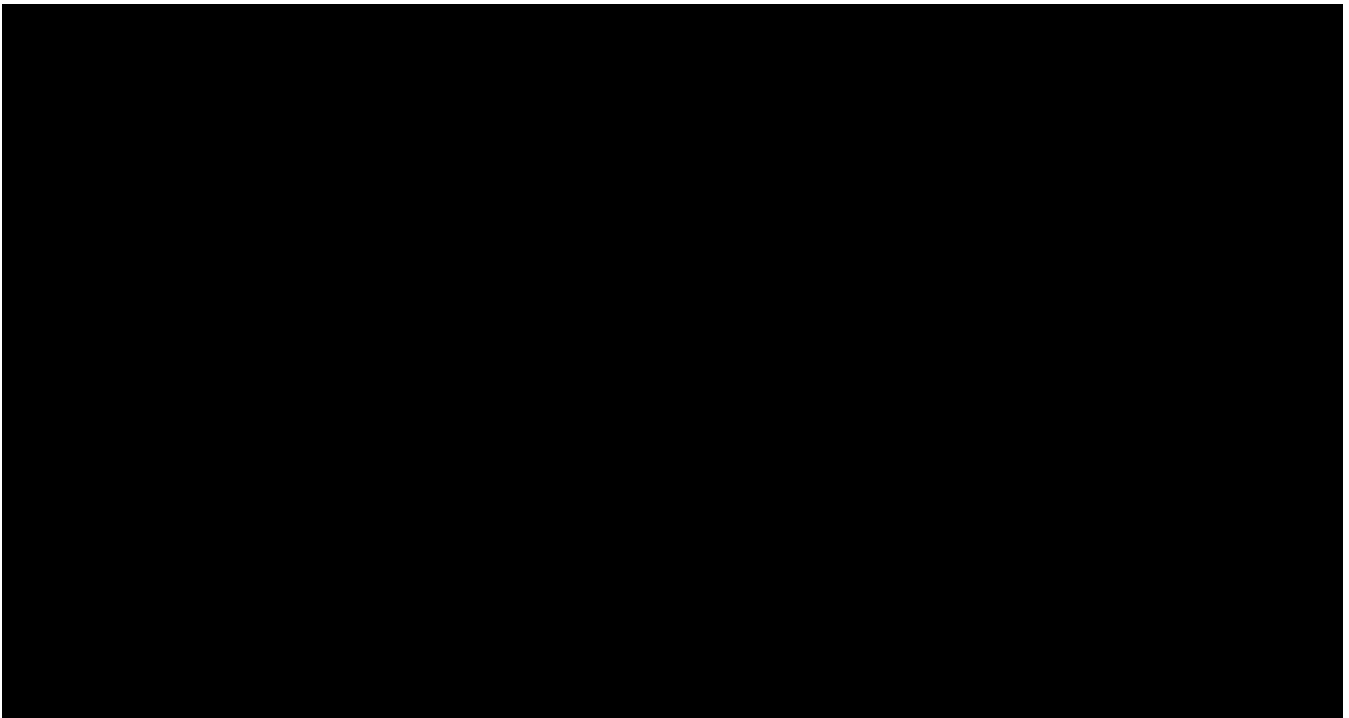


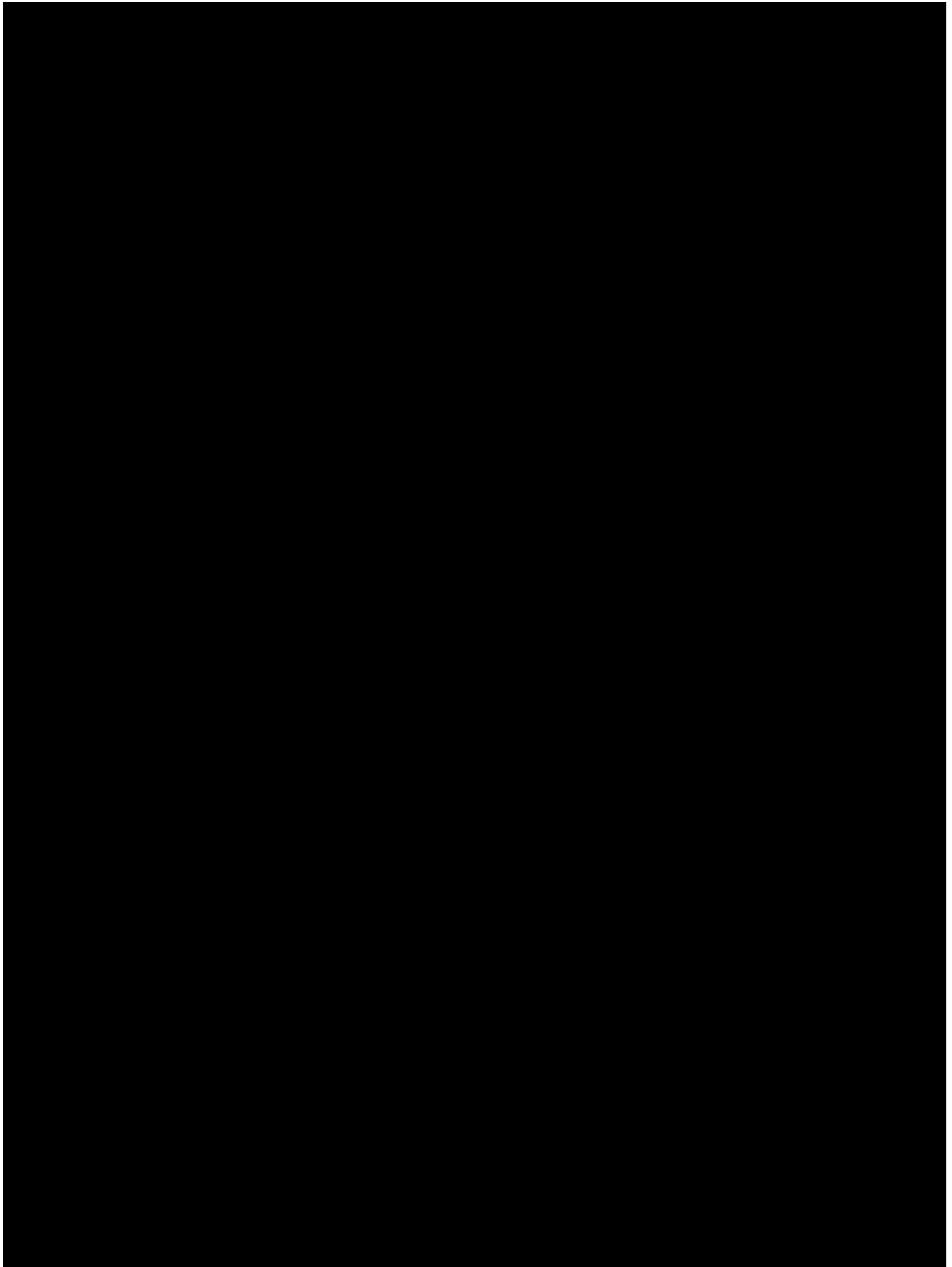


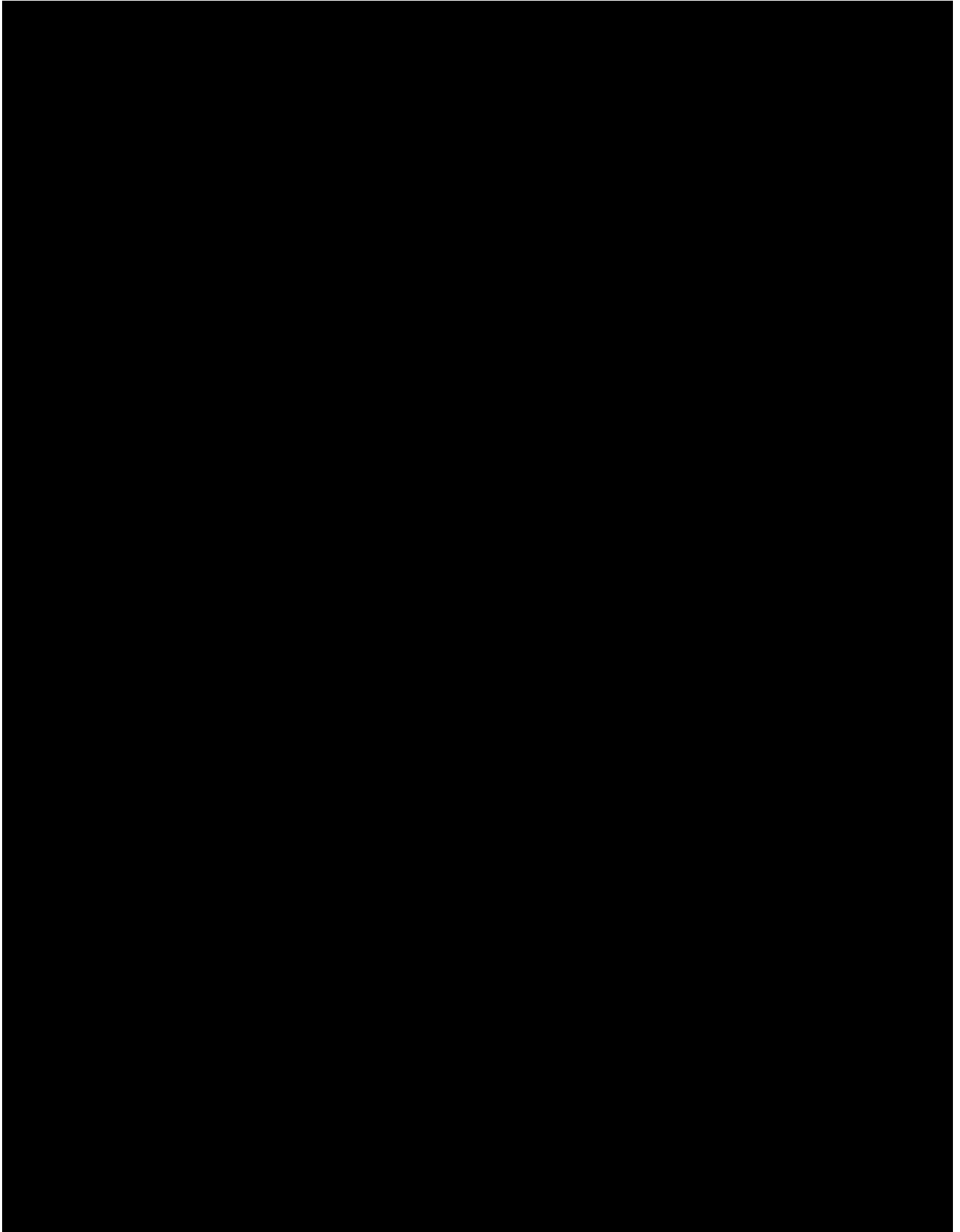


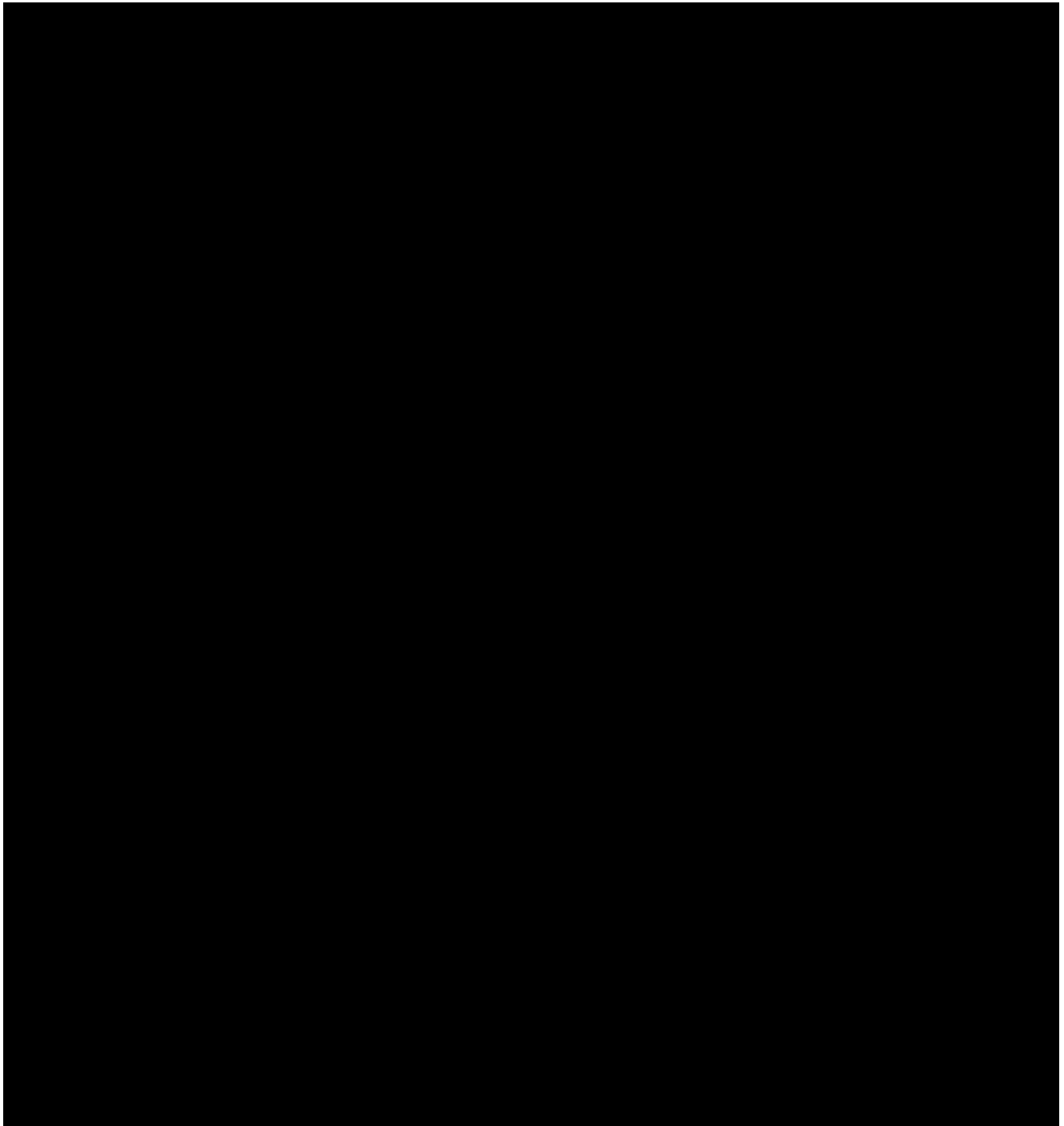
Describe your testing processes for the Solution in detail, specifically:

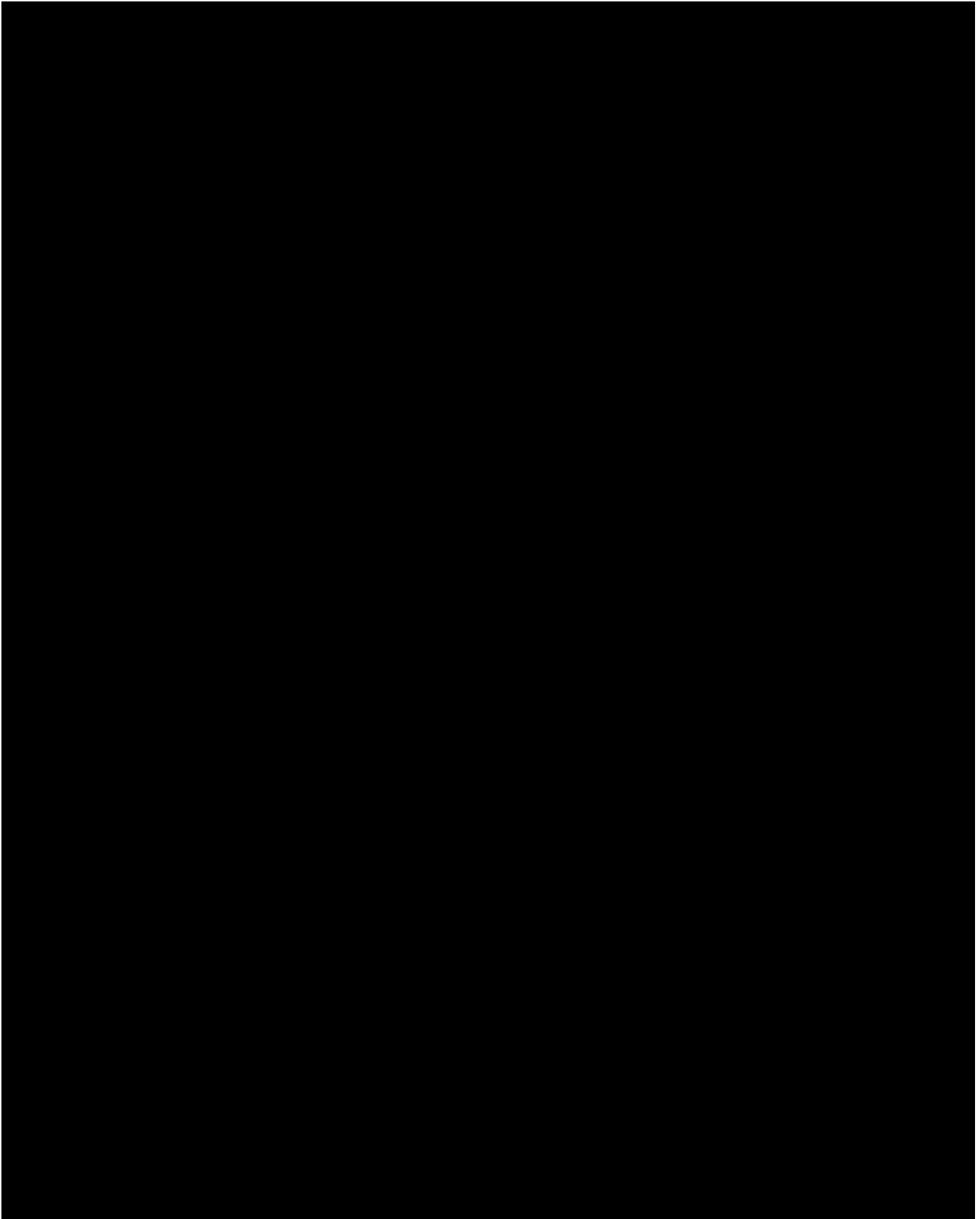
a. Your approach to conducting all types of technical testing needed prior to User Acceptance Testing, each release/deployment, including pilot deployment, and post-deployment validation.

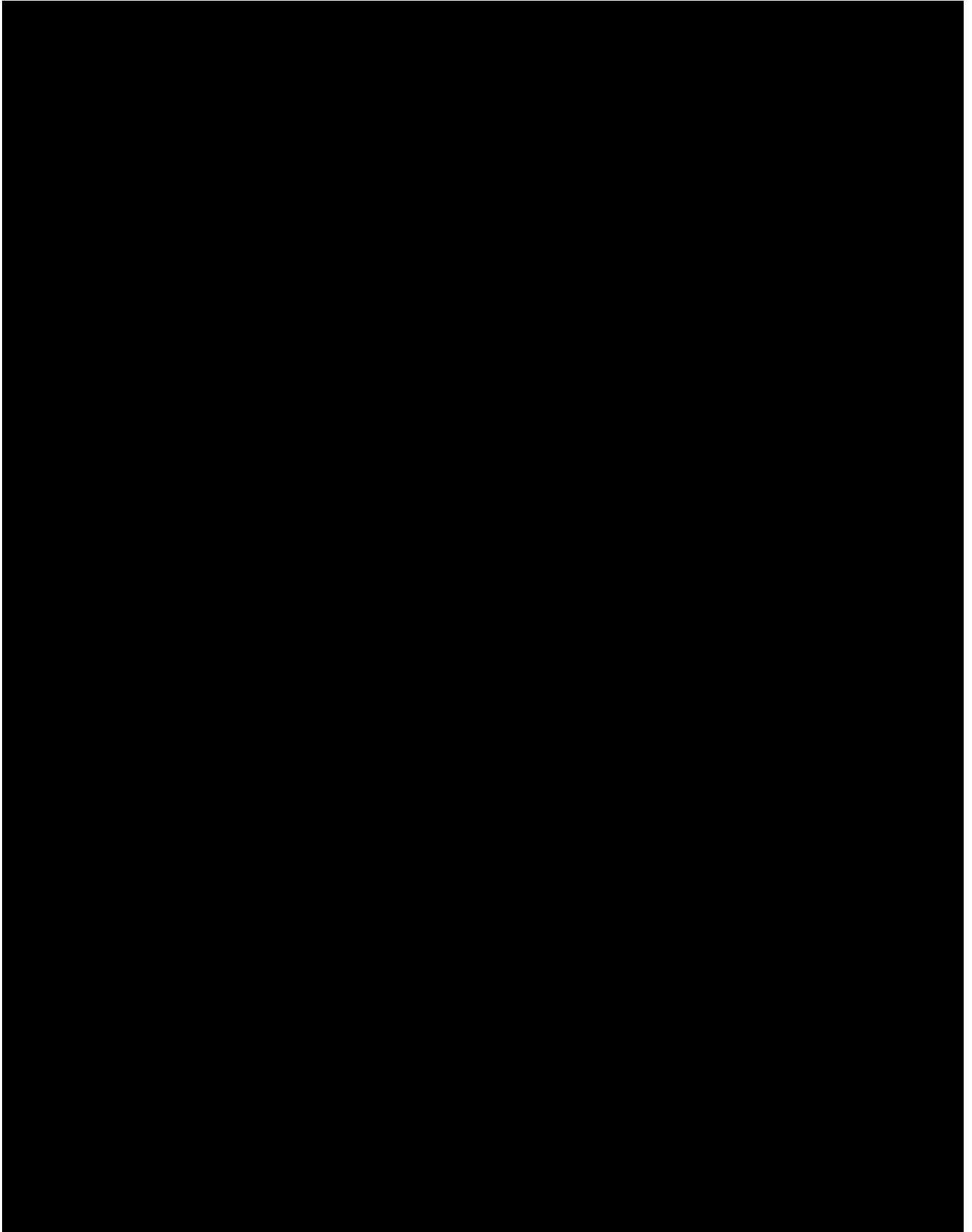


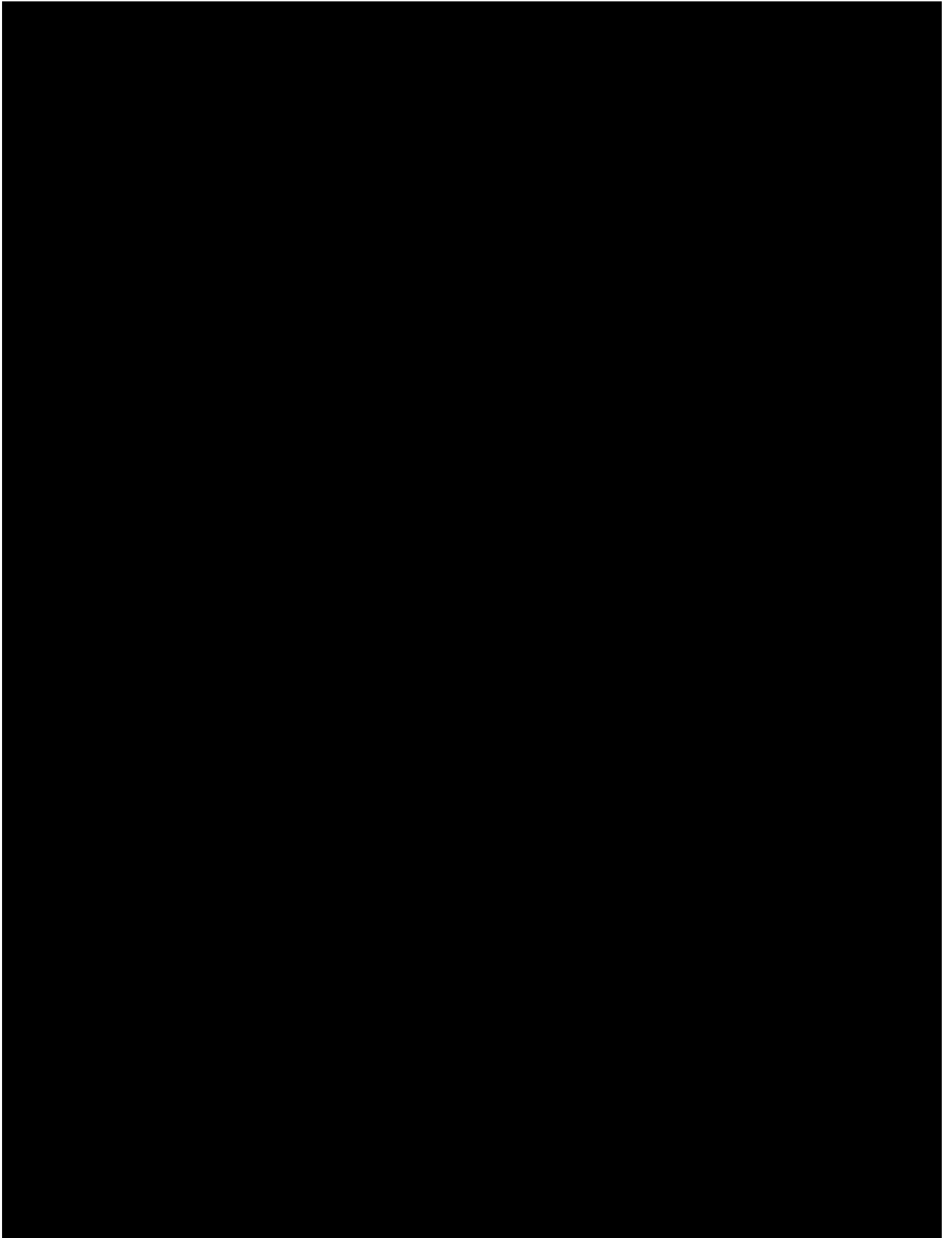


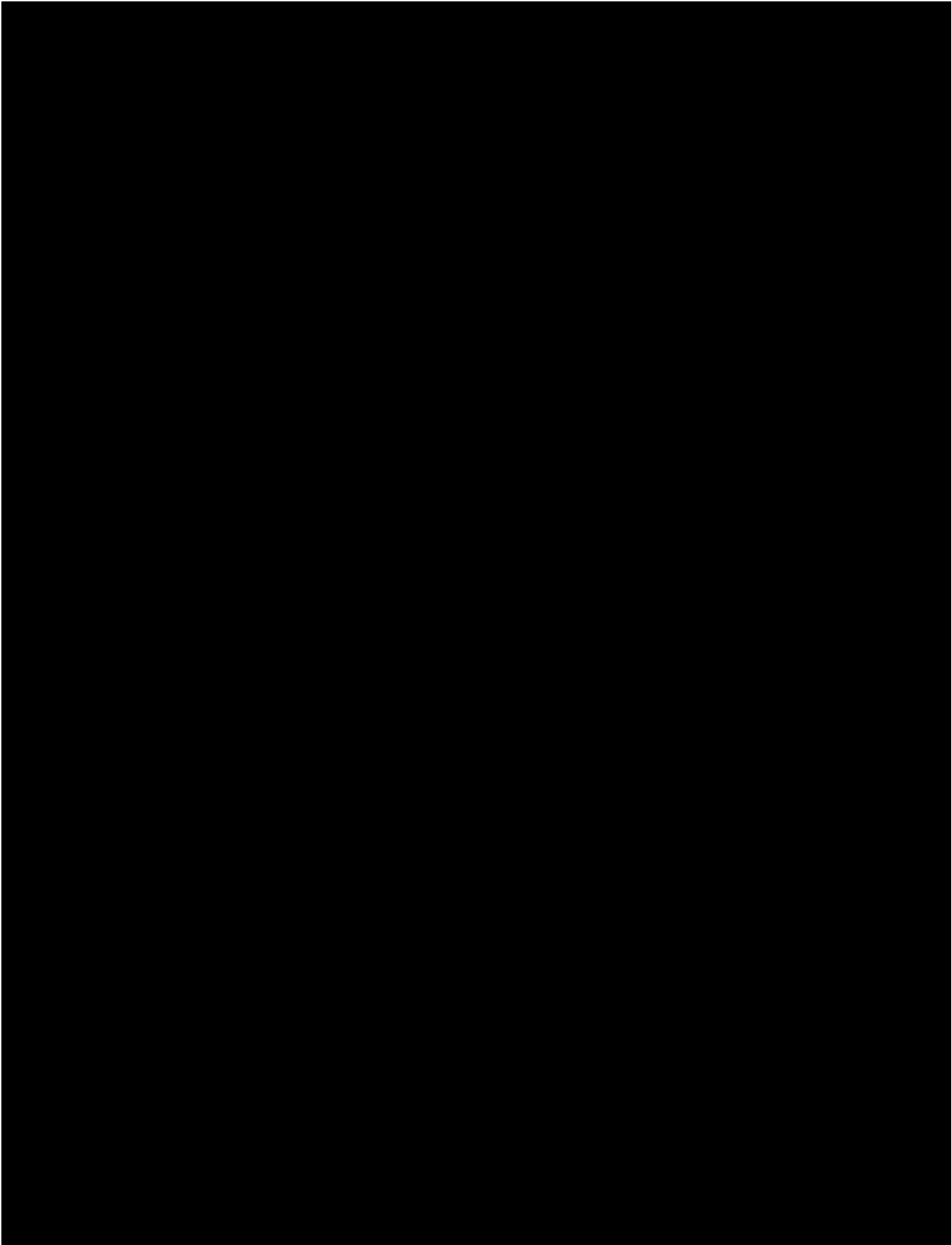


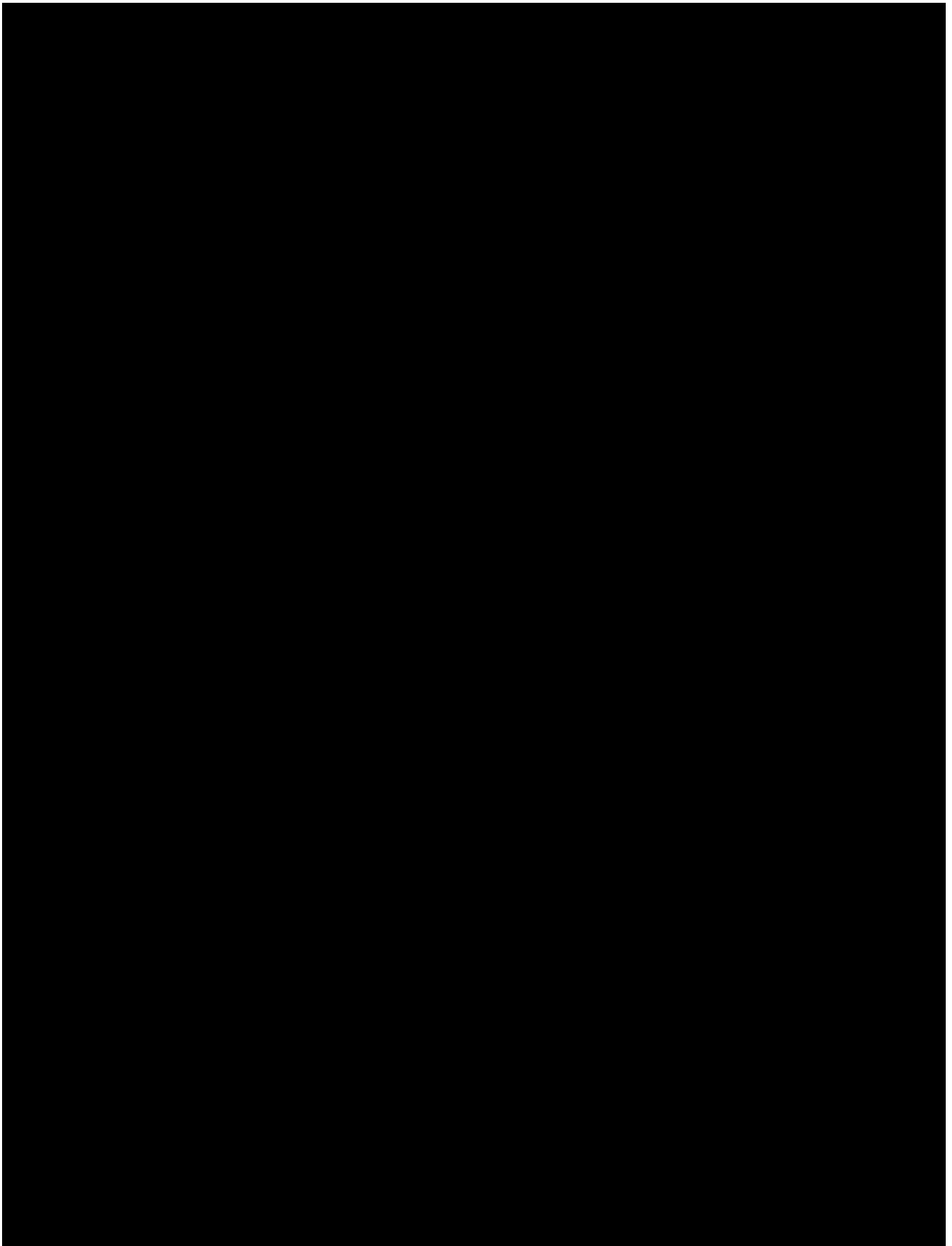


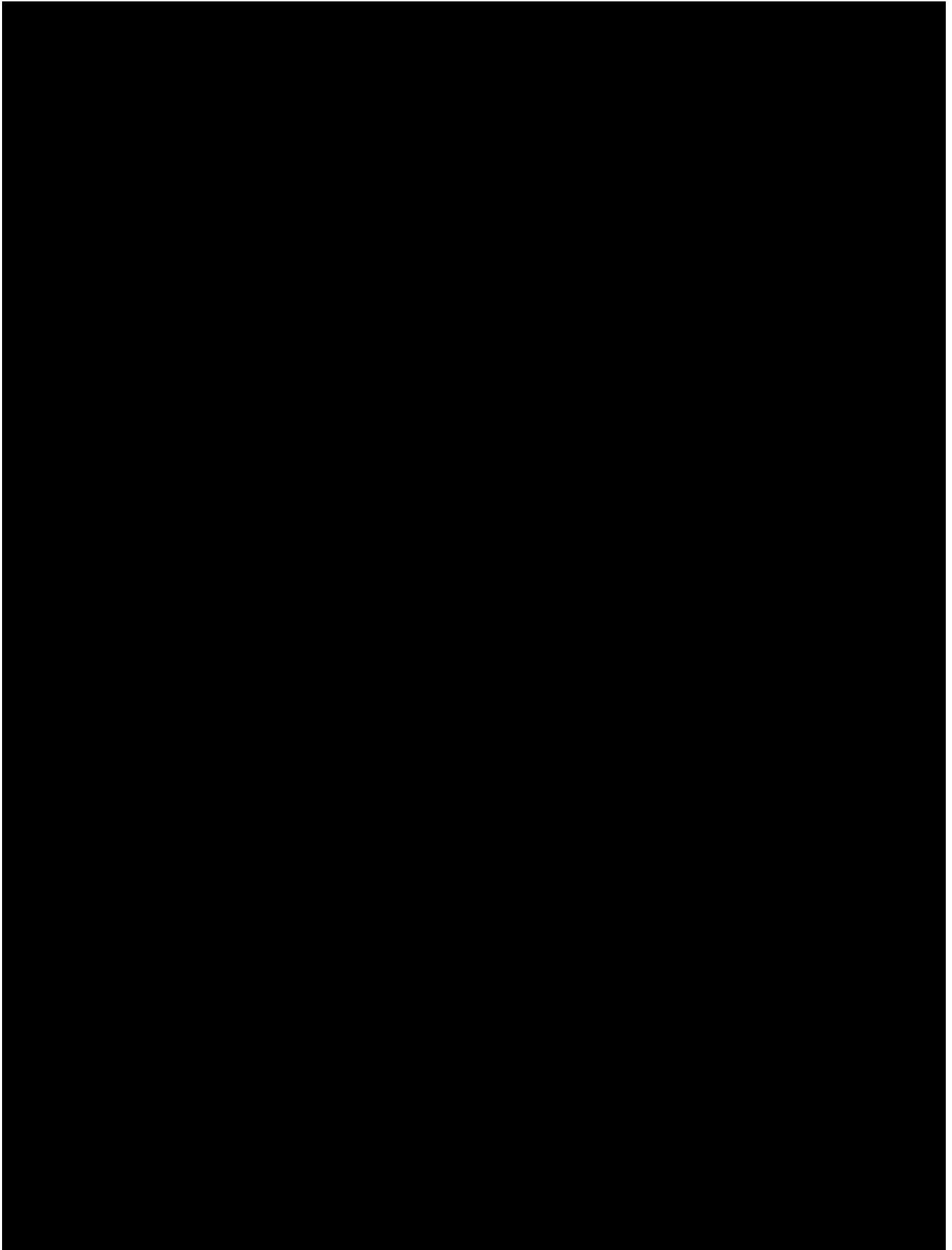


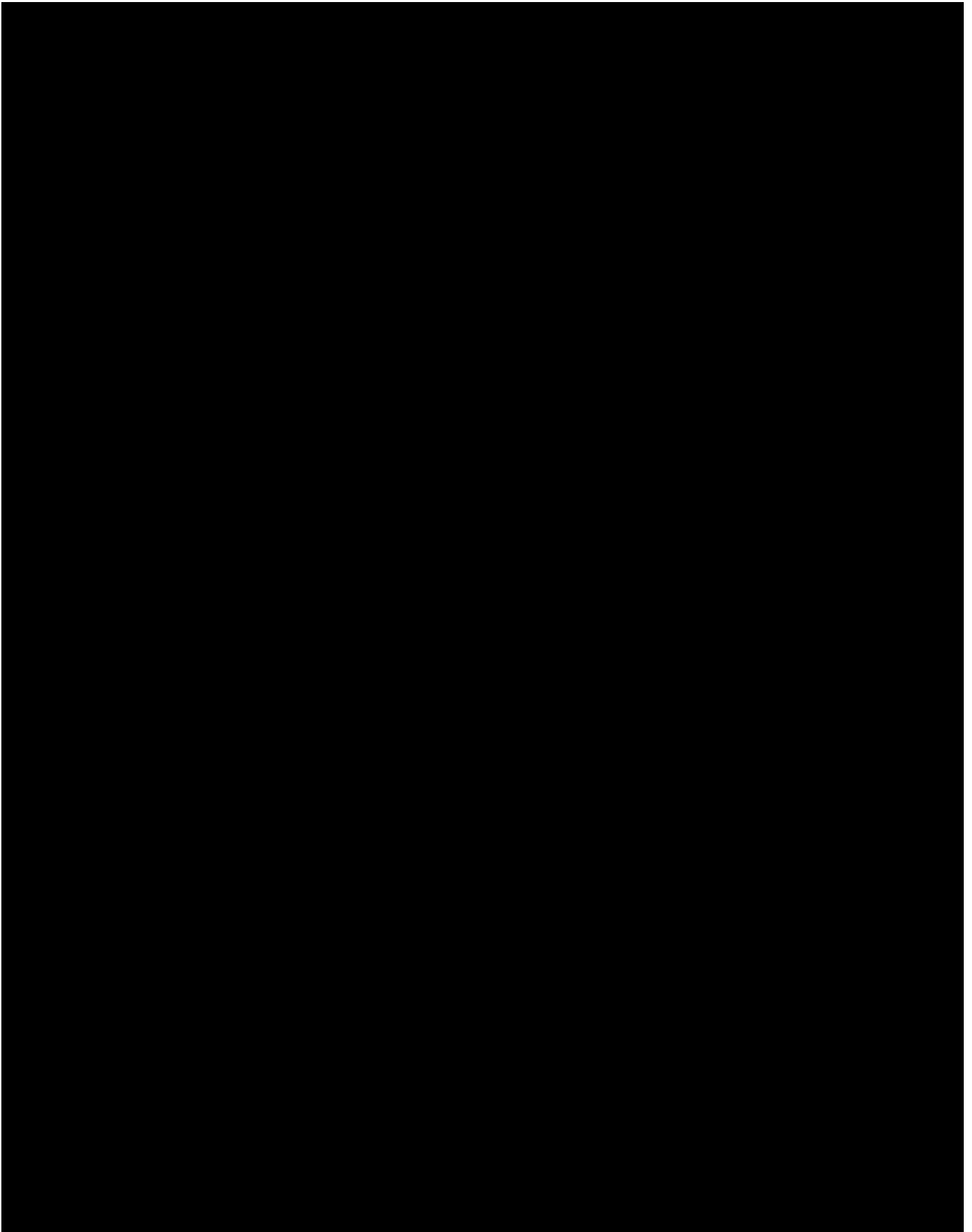


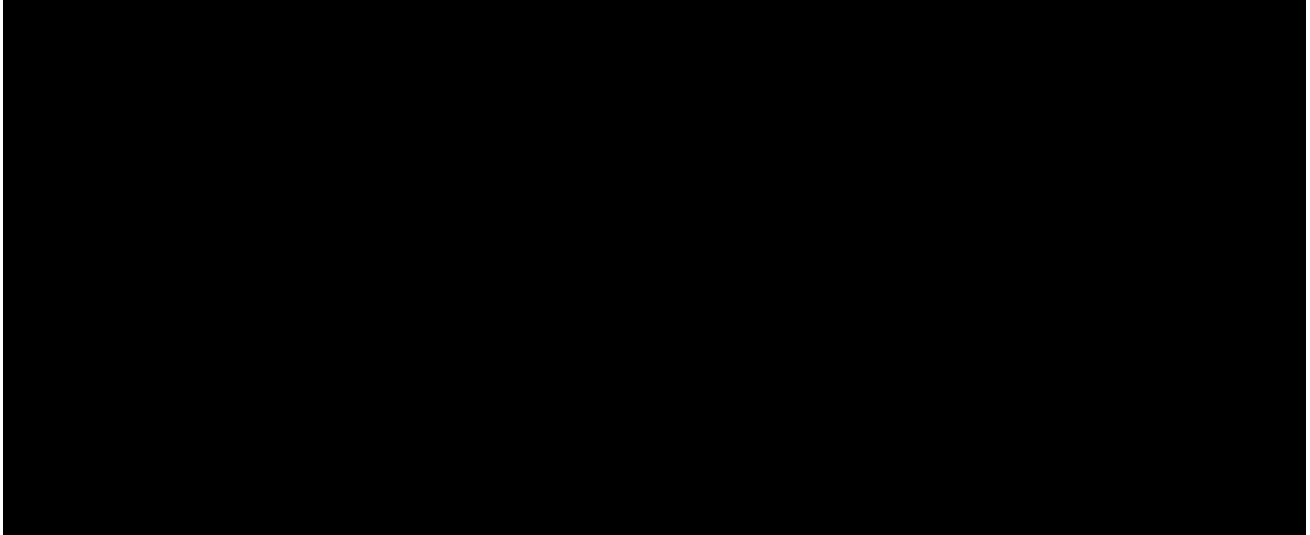








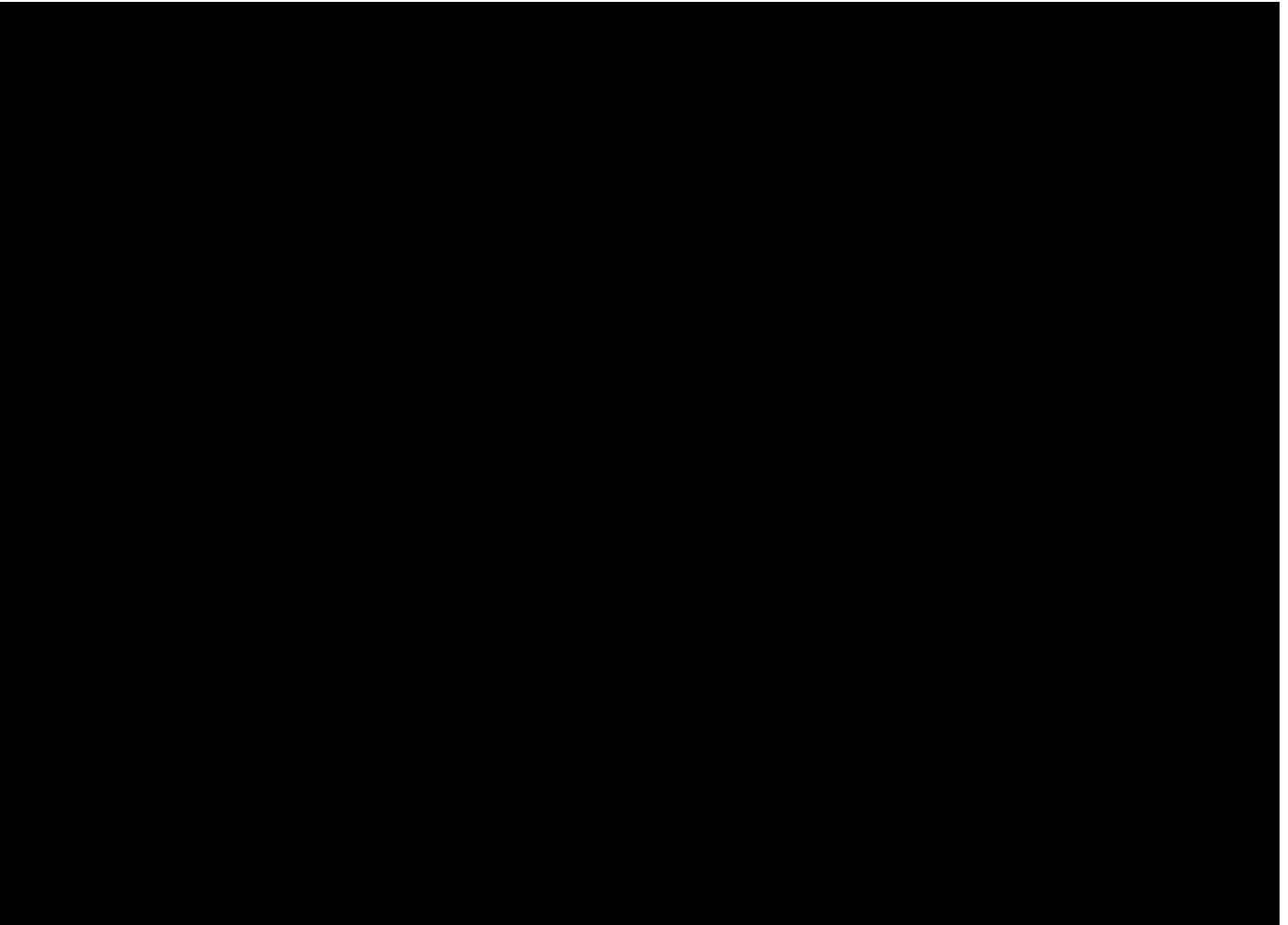


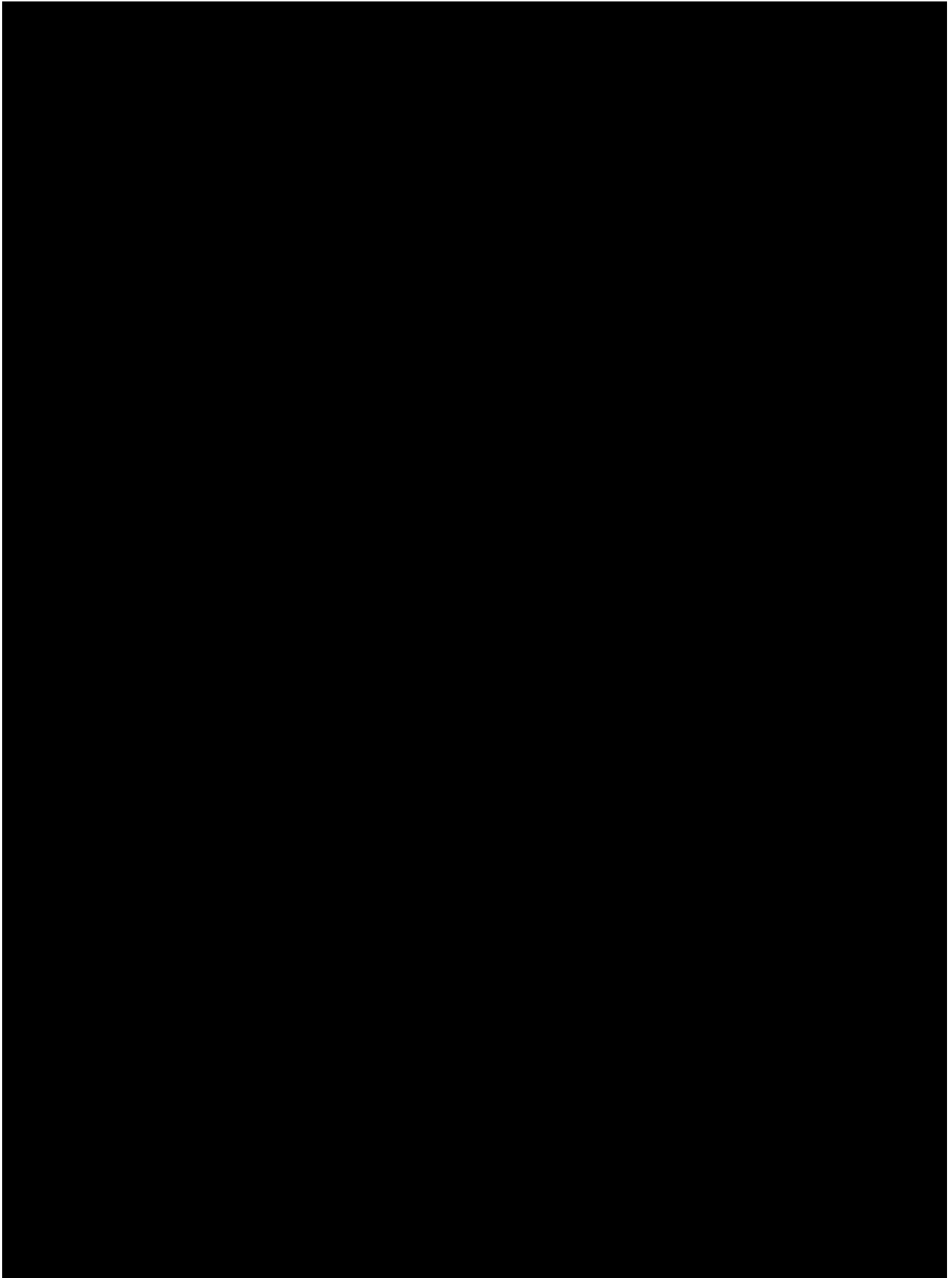


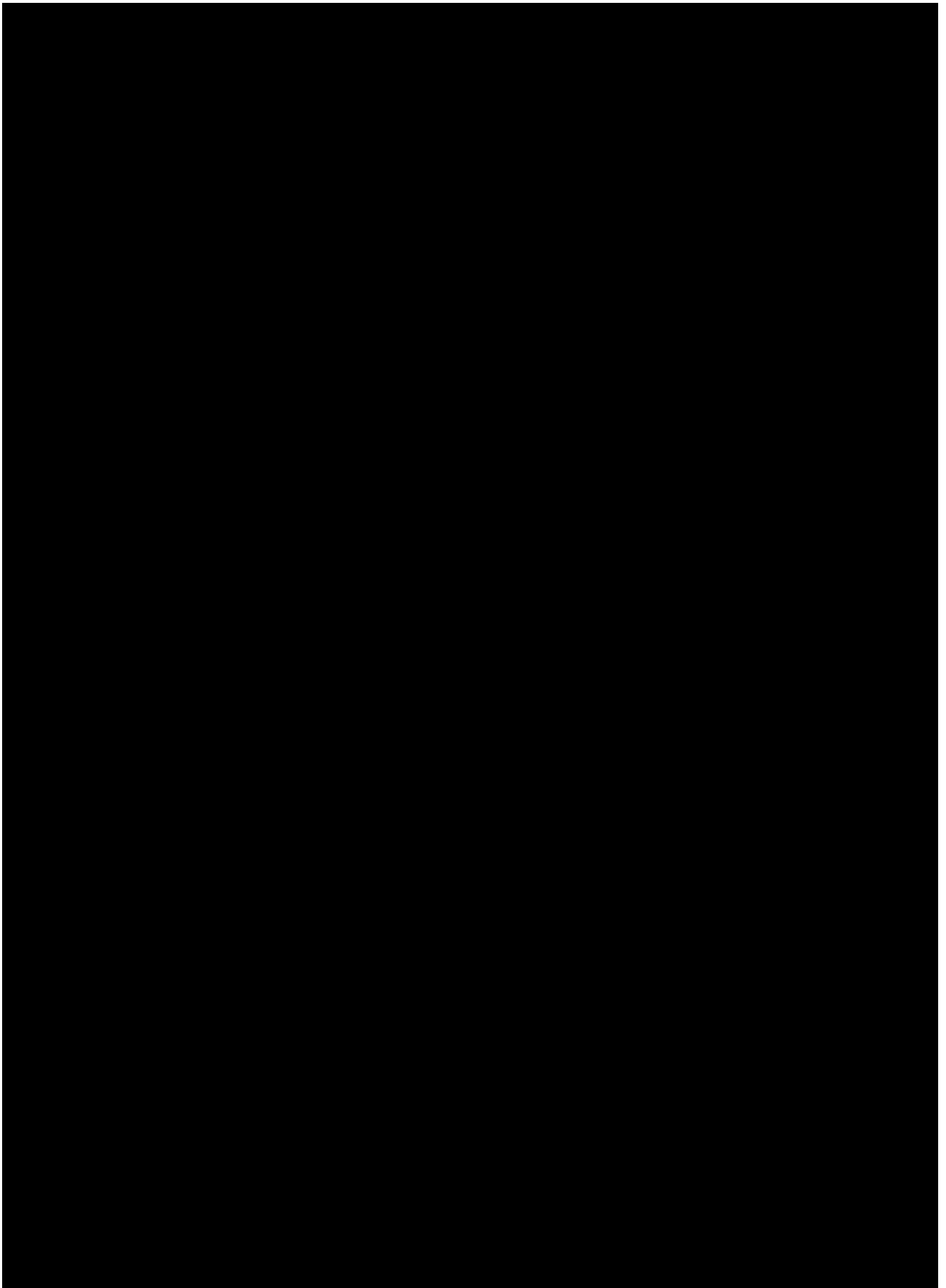
3.5.4 Training

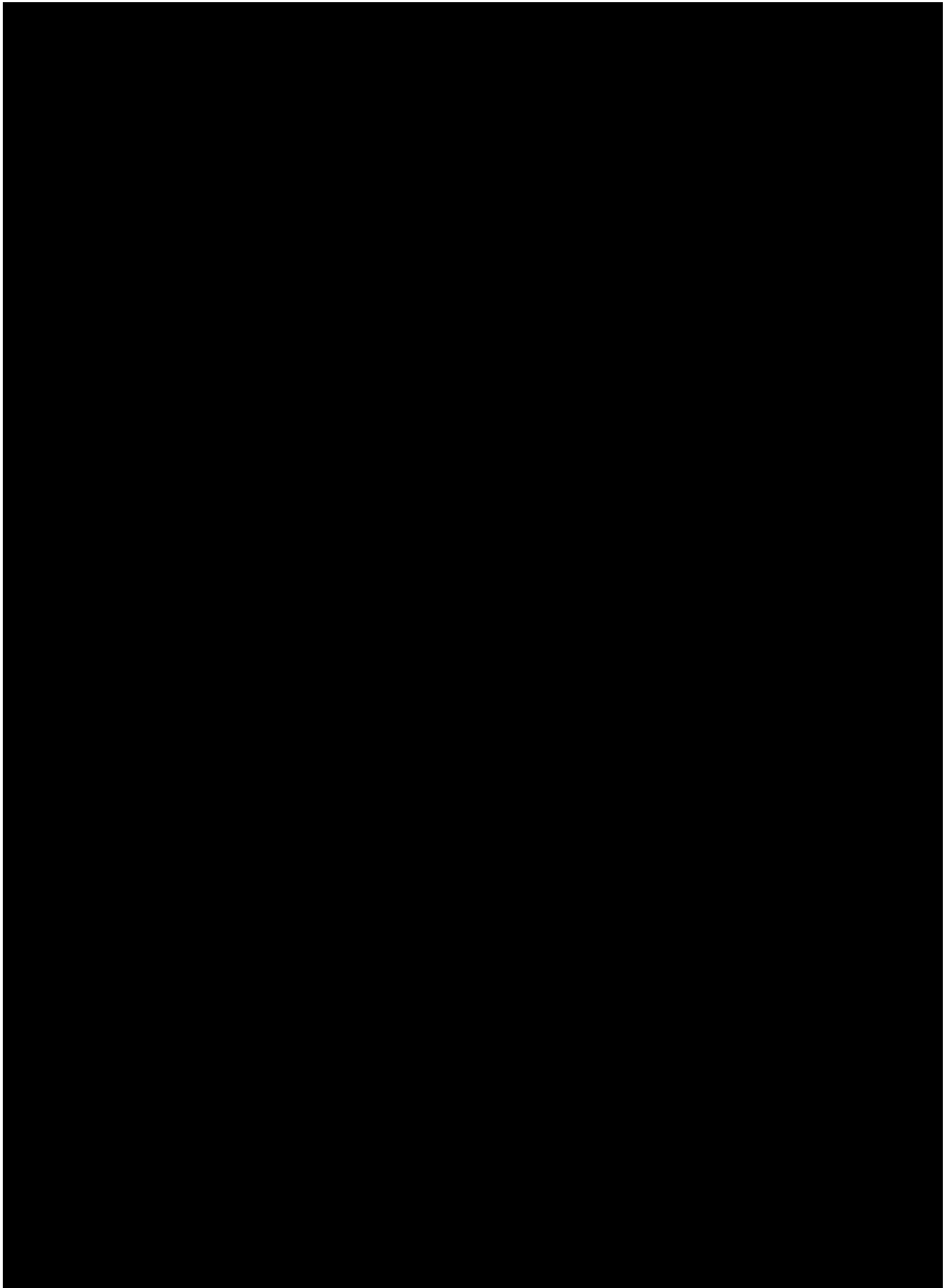
Describe your approach to training, identifying the points in your SDLC where training will occur for each type of training that you will provide to User Acceptance Testers, pilot users, end users, State Trainers, and State IT support staff. Include in this description:

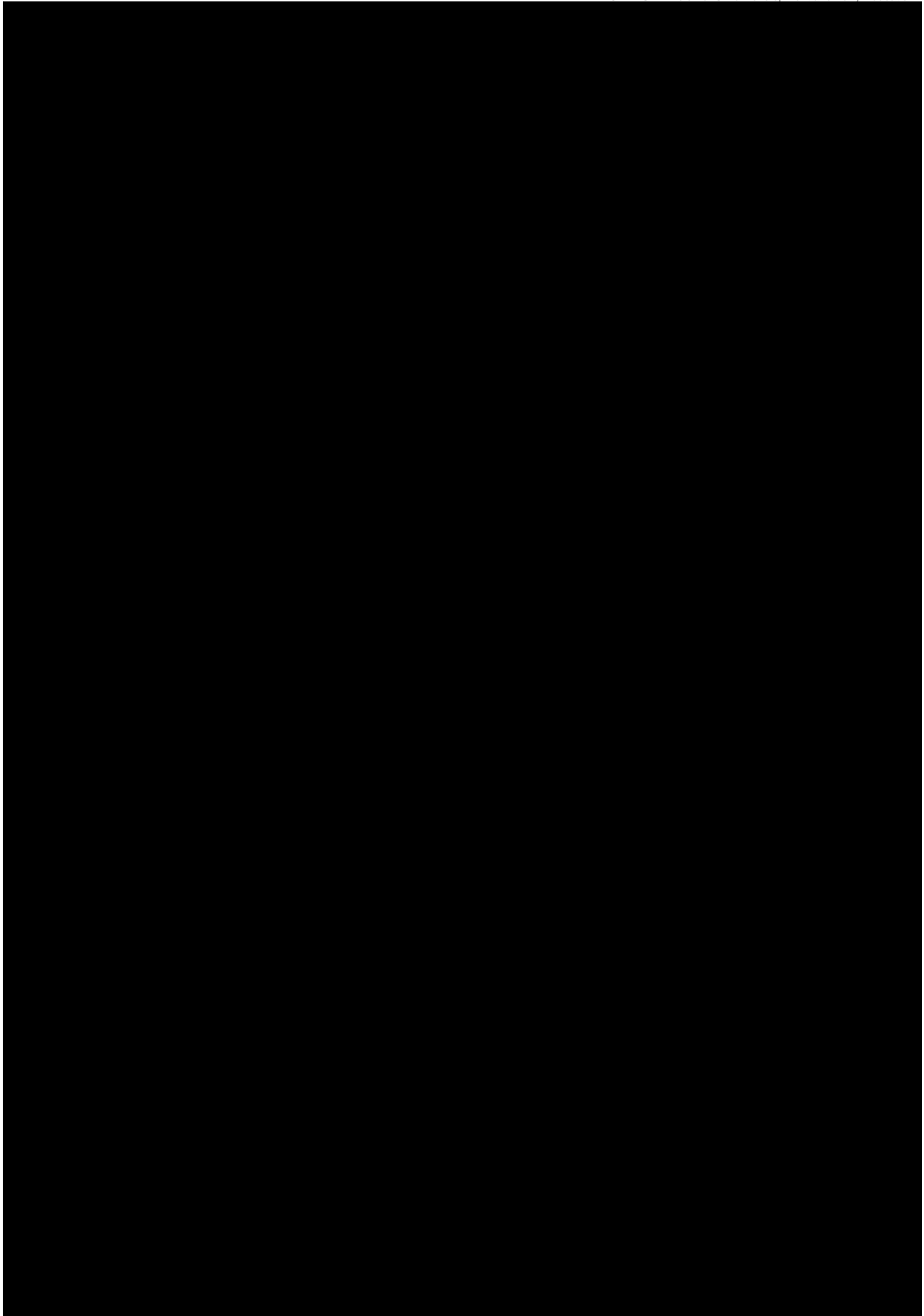
a. The training content that you will provide for the Solution, including the approach for in-person, remote, or pre-recorded training. Reference Section 3.5.2.2 and Attachment J, Minimum Content for Project and O&M Deliverables. for details regarding the Agency's training documentation needs .

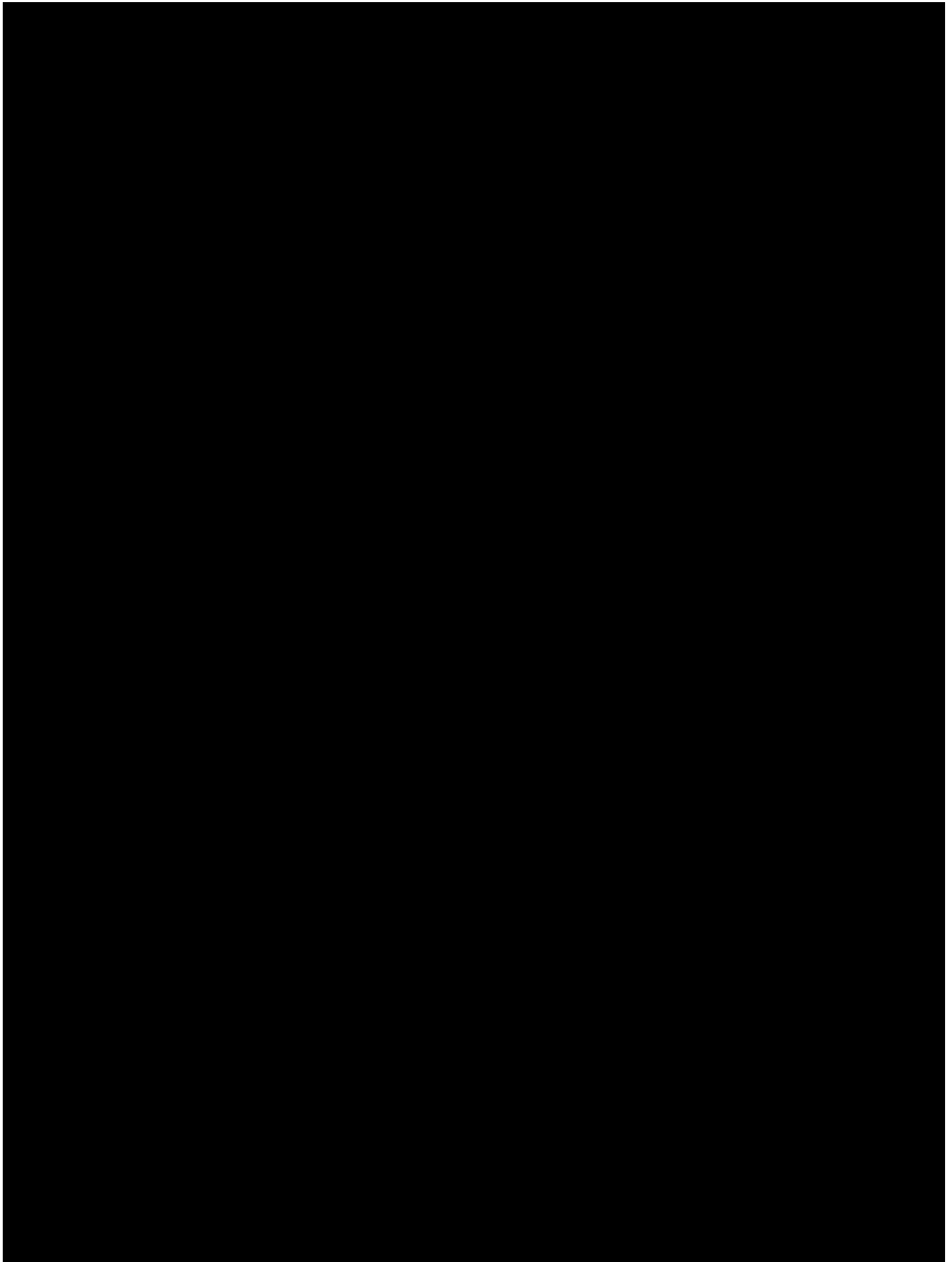


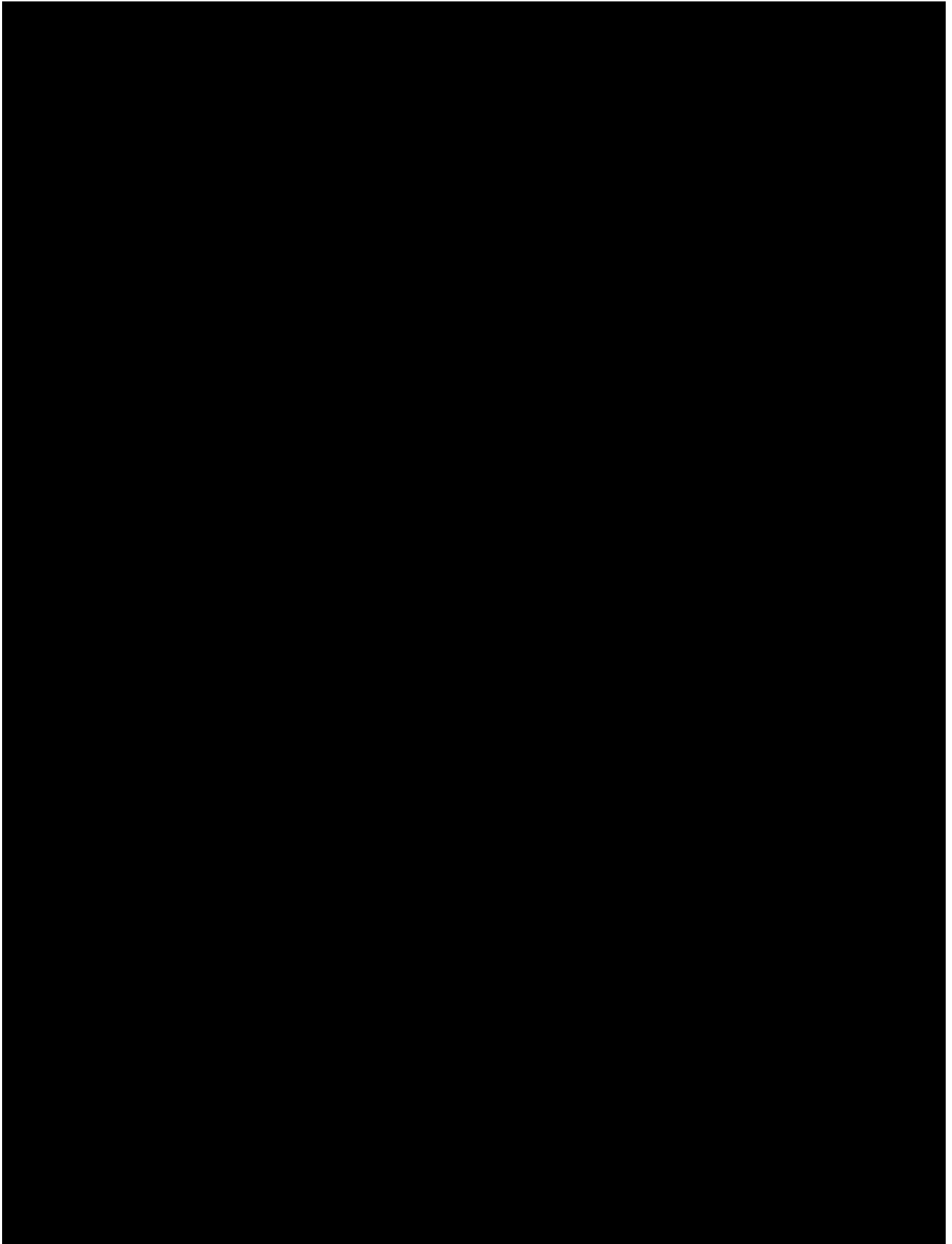


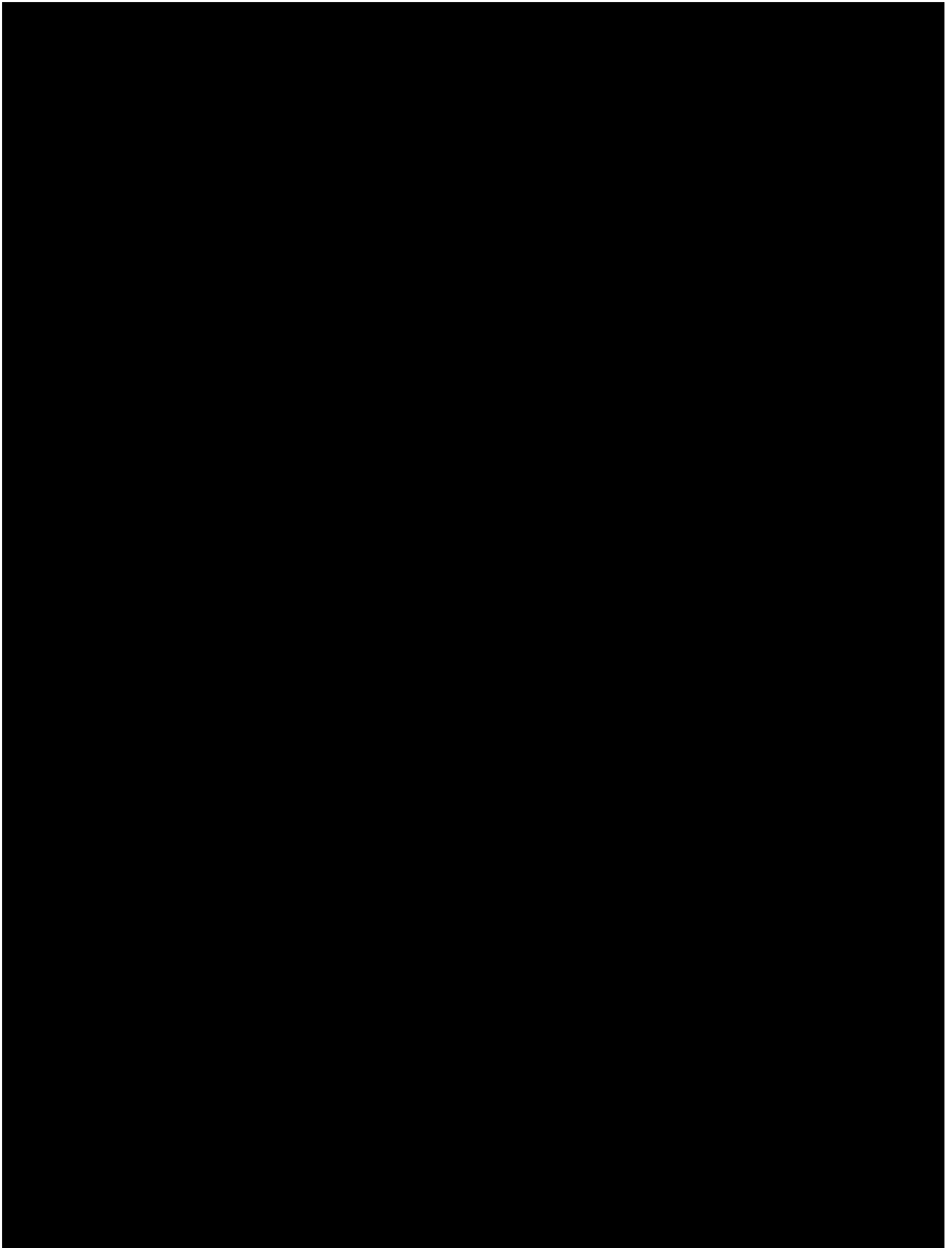


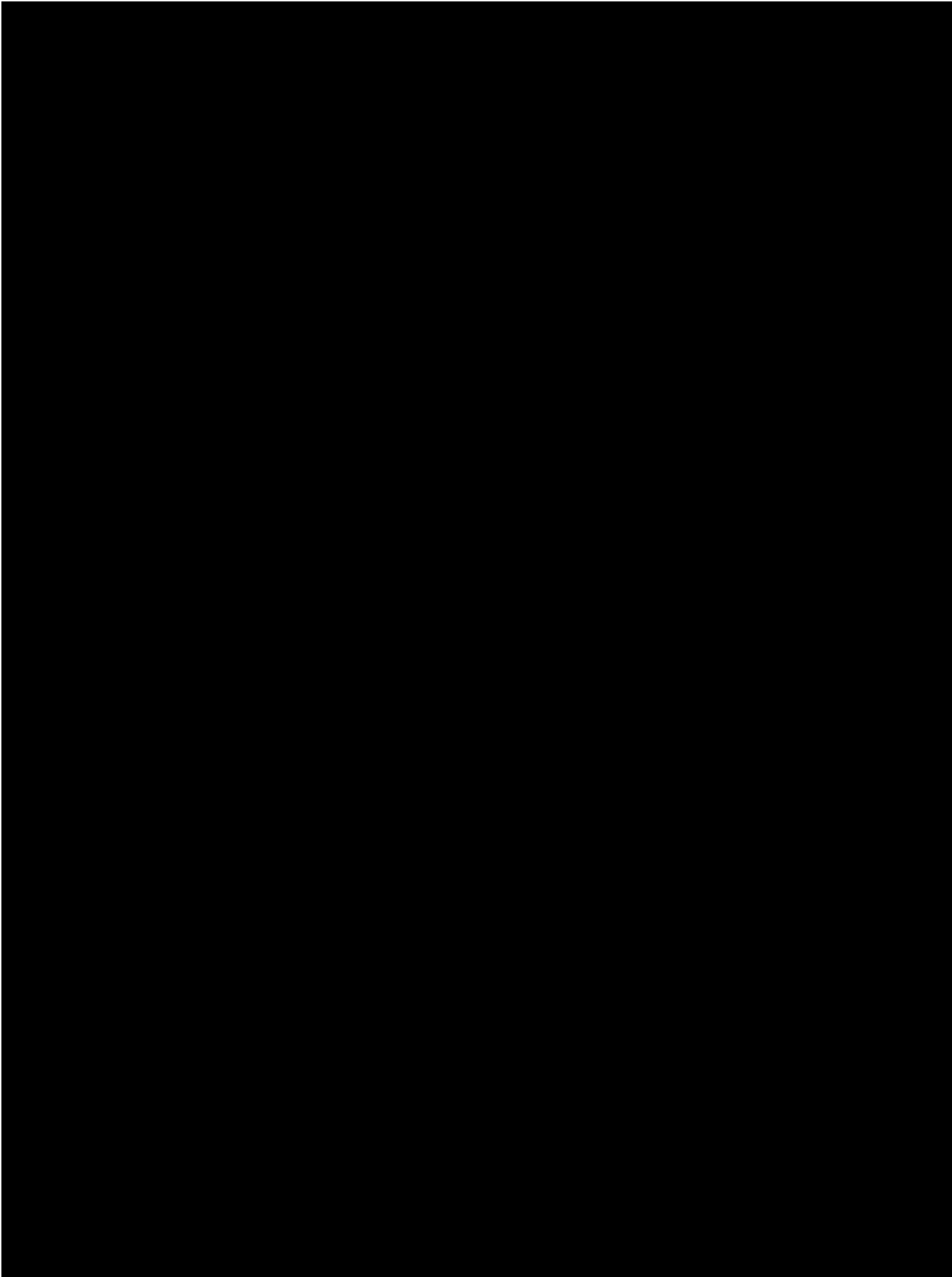


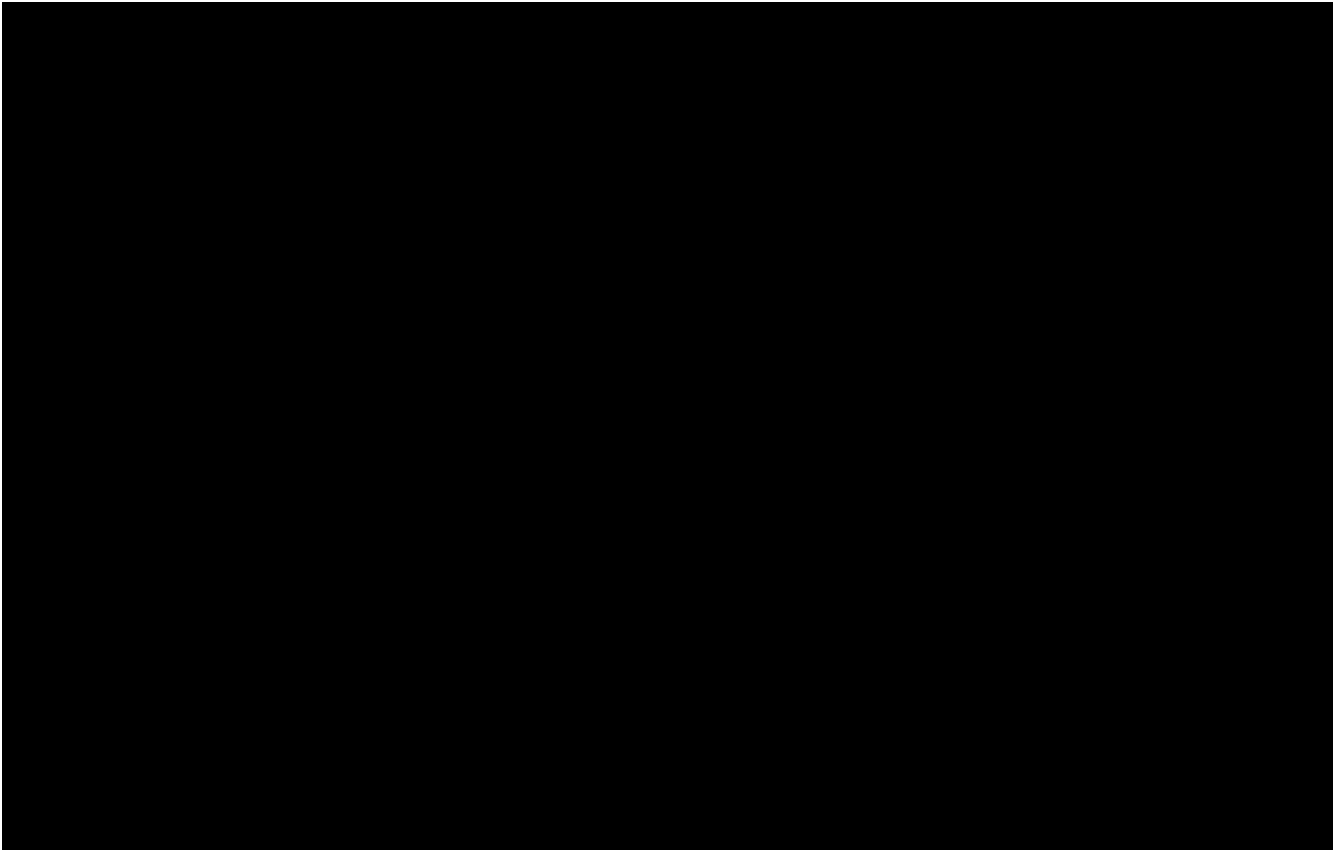






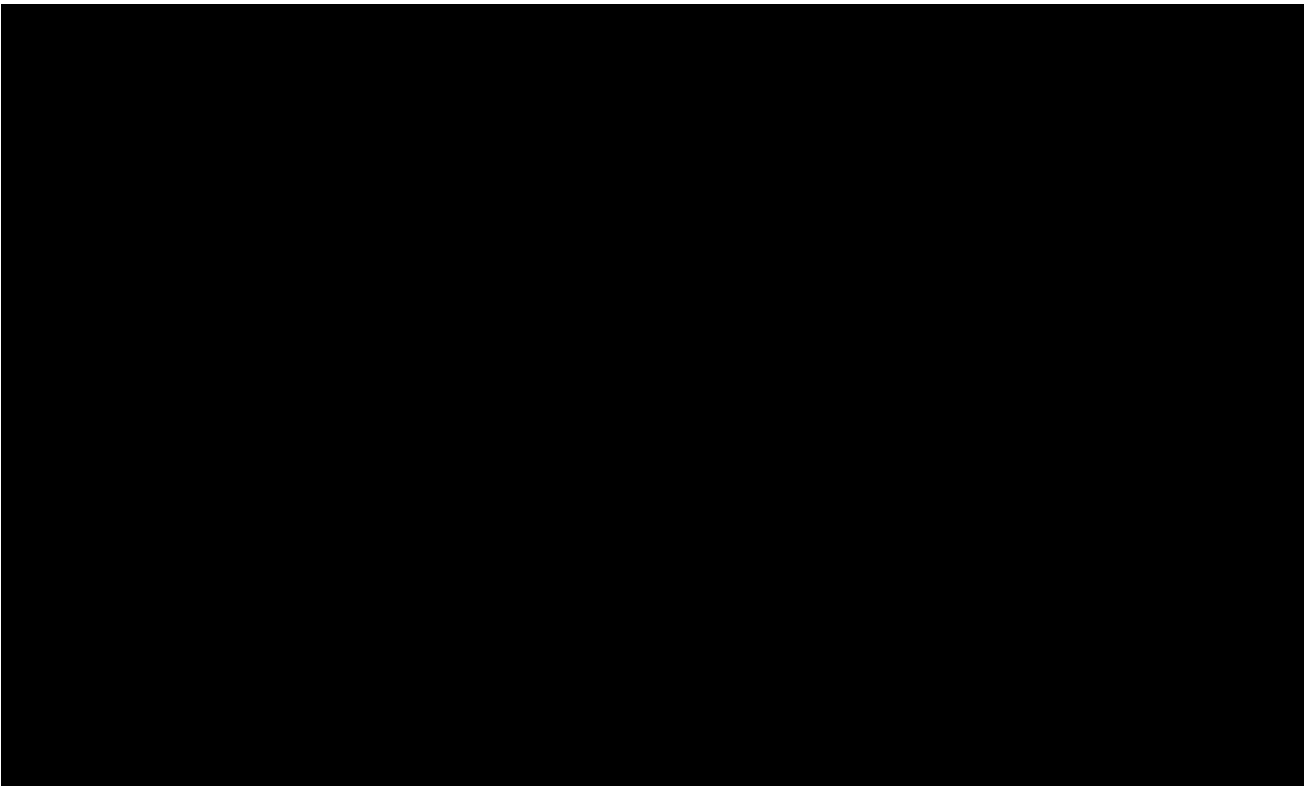


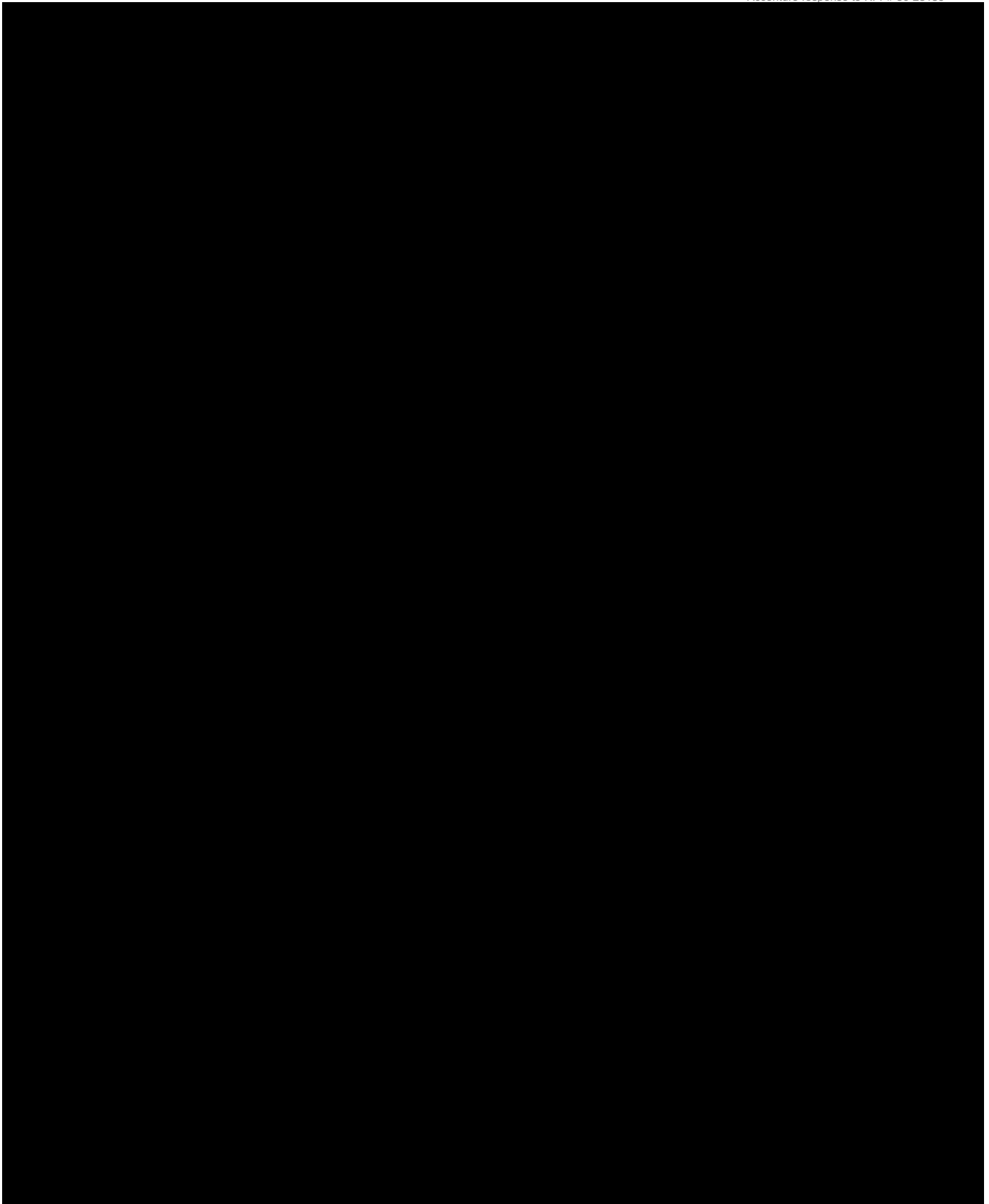


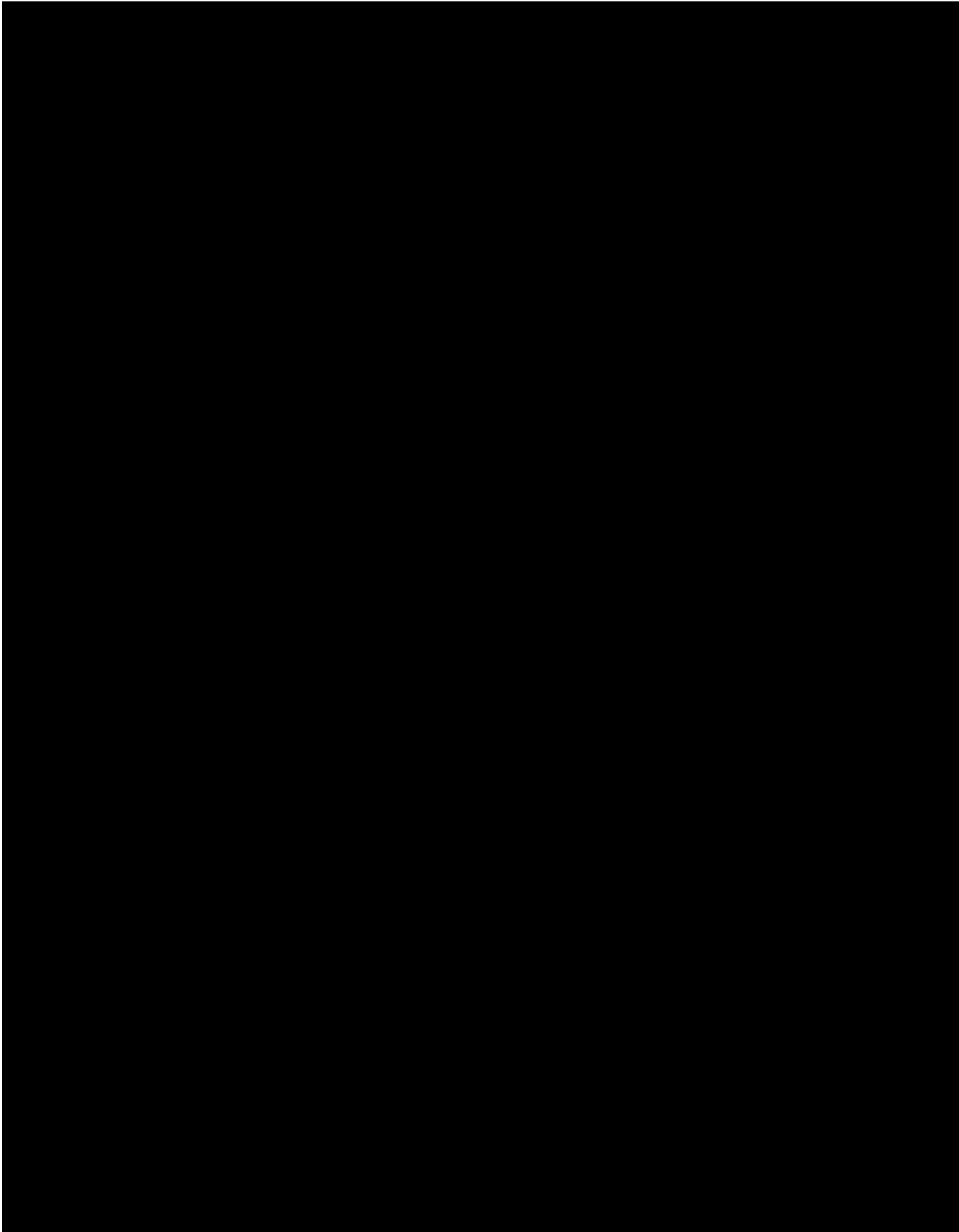


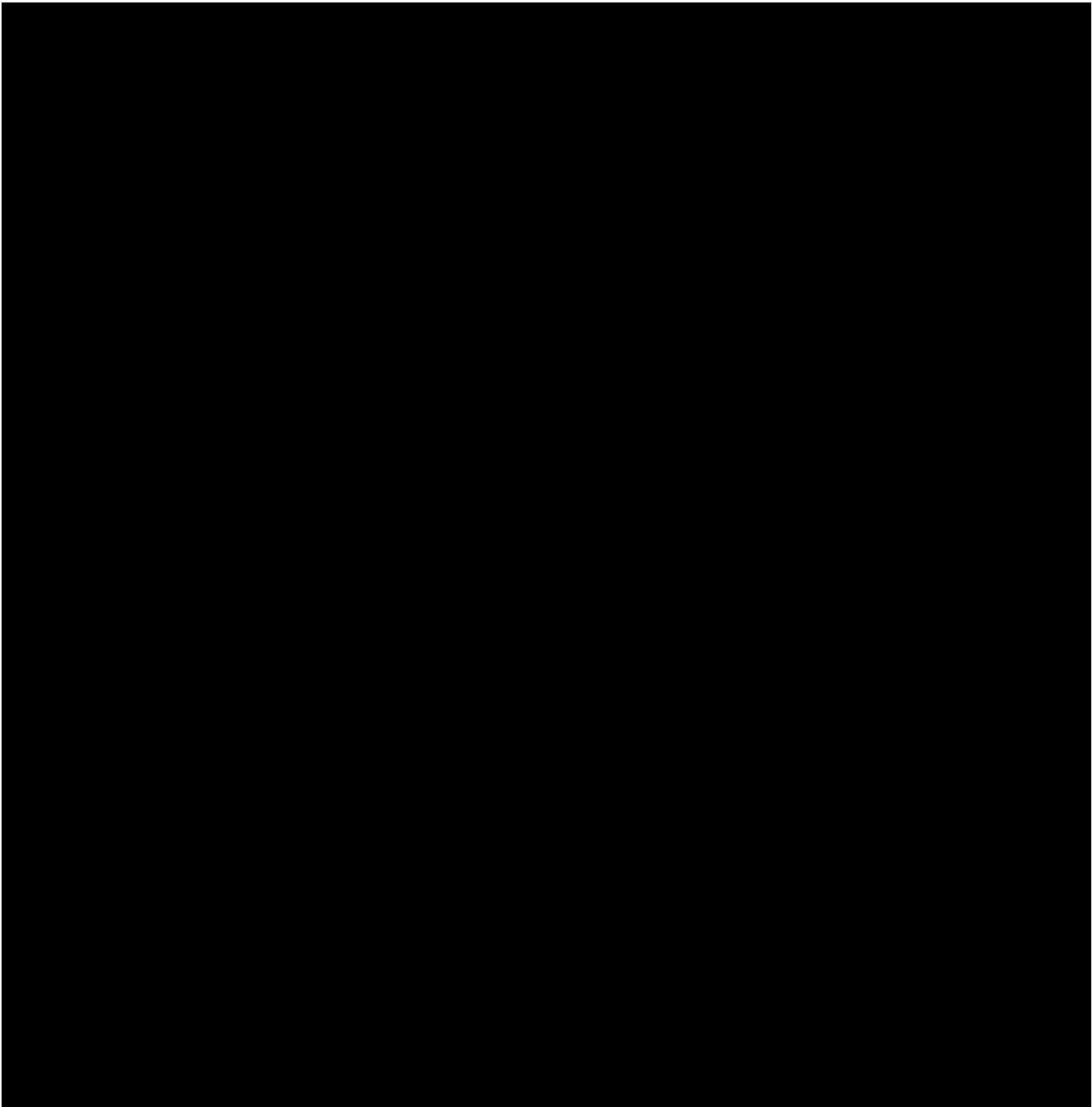
3.5.5 Data Conversion and Migration

Describe the Vendor's approach to converting and migrating data from existing systems (Regulatory (SQL), WORKS (Oracle), etc.) to the Solution. Include a list of all tools that will be used, and State resources required.









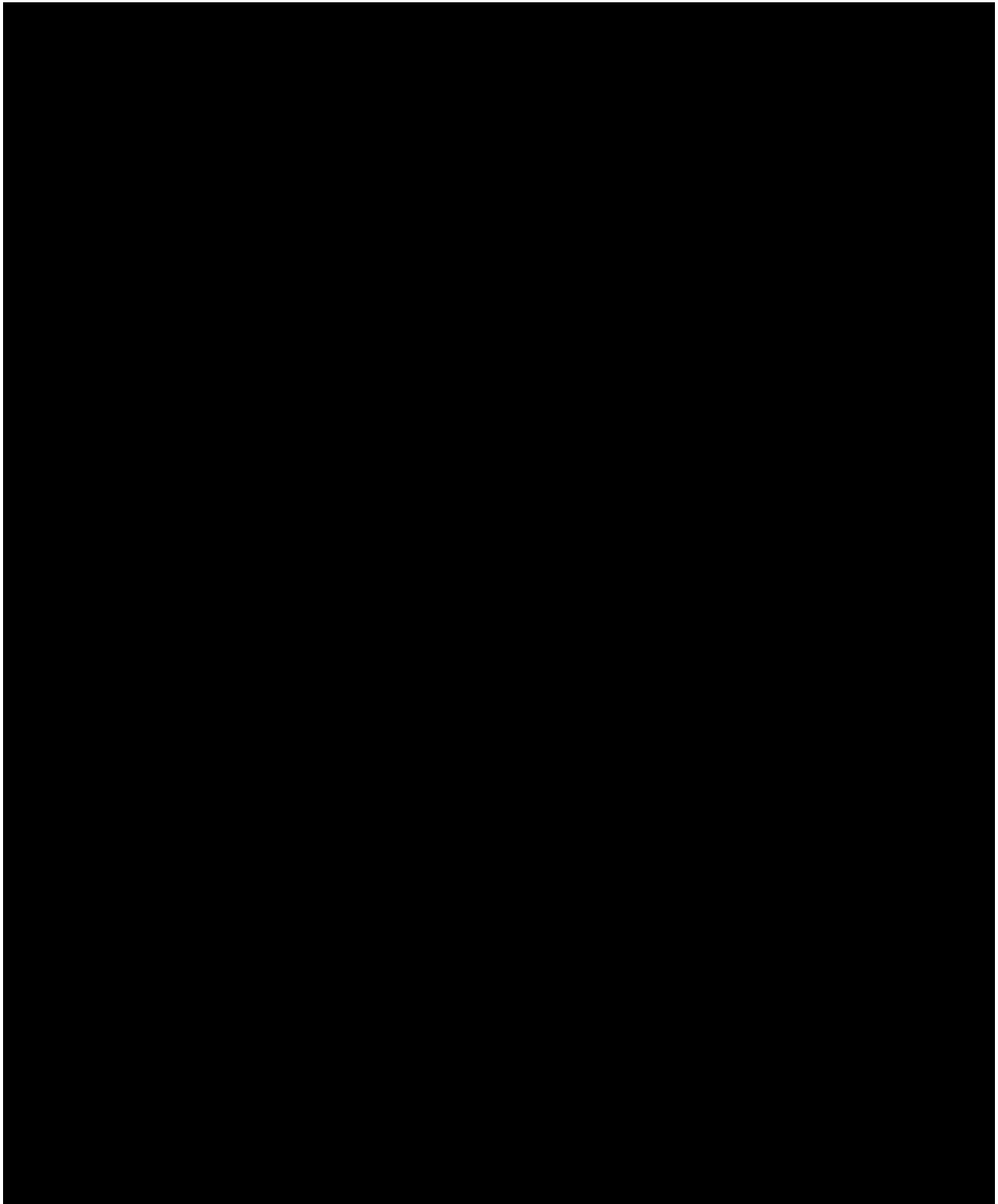
3.5.6 Operations and Maintenance

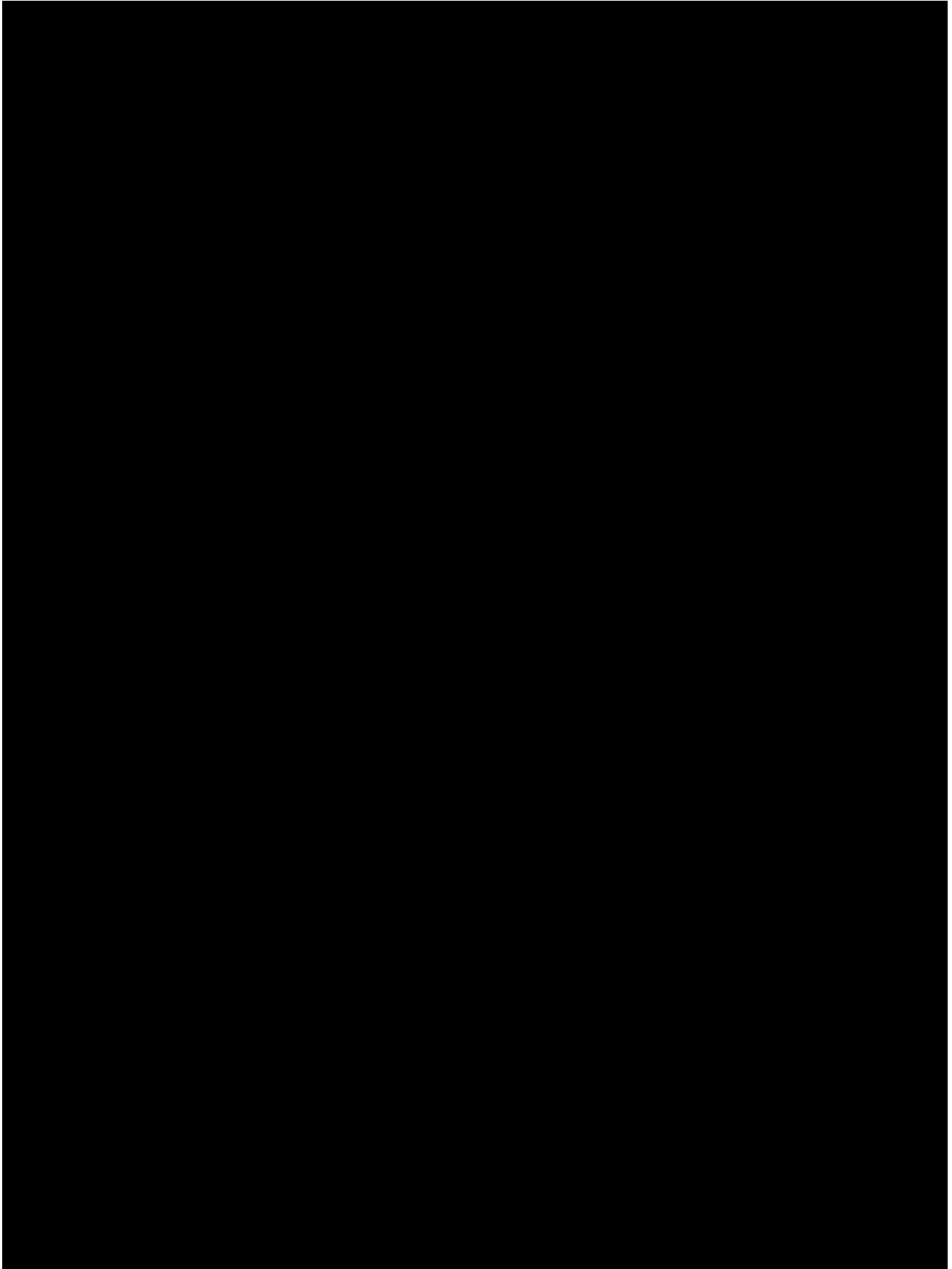
1. Vendor Approach to Operations and Maintenance

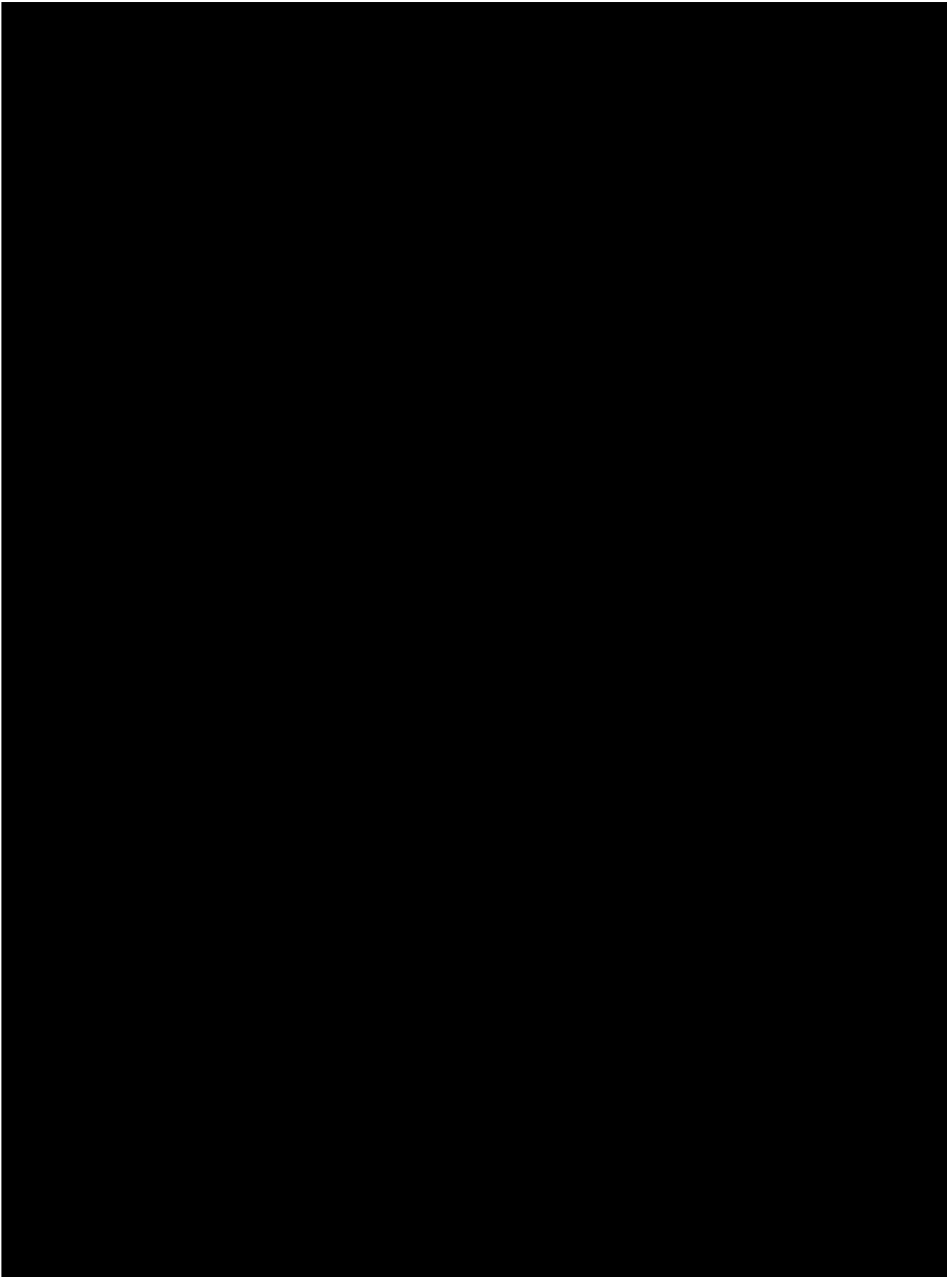
O&M will start after the Solution is deployed and the Vendor has obtained documentation of Agency Acceptance of the Stabilized Solution (i.e., the Stabilization Period has been successfully completed). The Vendor, when offering a Vendor-hosted Solution, will maintain the hardware and operating systems needed to host the Solution and updating the Solution with product patches and new releases. Describe the Vendor's plan to perform/provide all O&M tasks/Deliverables. Reference 3.5.2.2 and Attachment J, Minimum Content for Project and O&M Deliverables for Deliverables that are to be maintained during O&M. Include a description of how the Vendor will do the following:

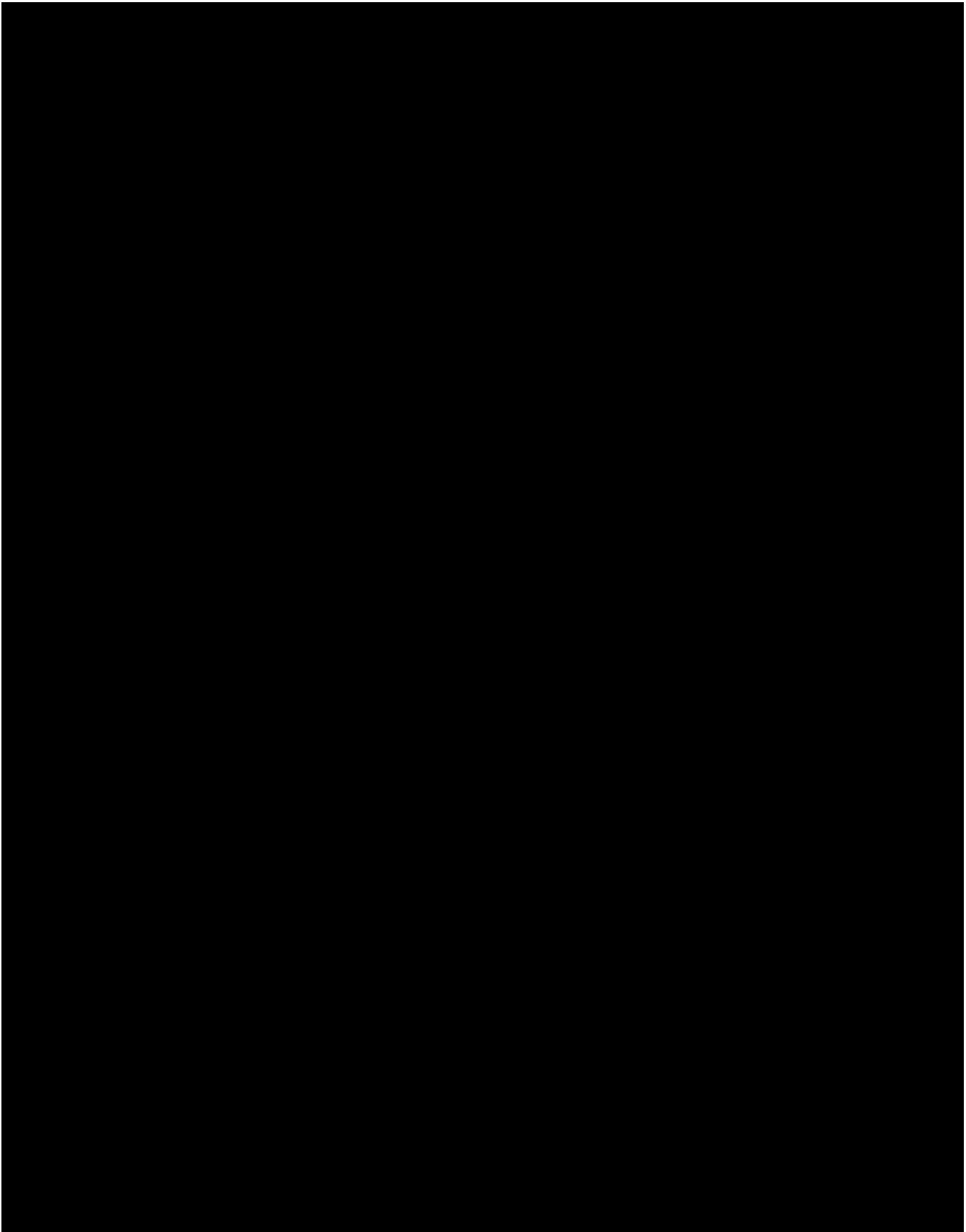
- a. Describe how you will provide ongoing maintenance and support for the Solution. This includes, but is not limited to, periodic updates based on new product versions.
- b. Provide a mechanism for the Agency to request Changes to the Solution and report Defects.

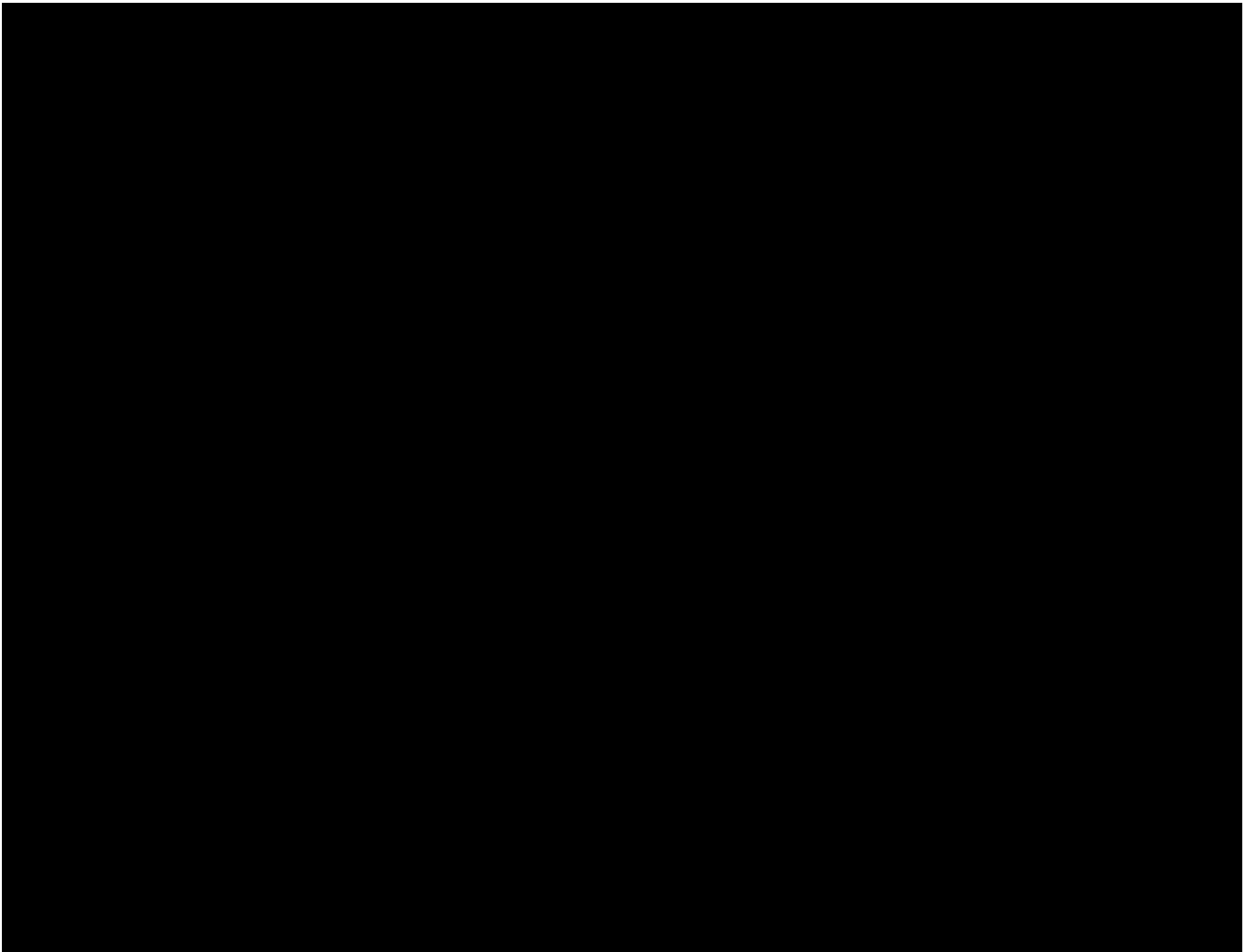
- c. Maintain a tracking system, at no cost to the Agency, to track all requested Changes and reported Defects, their status, expected resolution time, testing results, and final resolution.
 - d. Provide the Agency with the status of releases, Changes, and Defect resolution in a format specified by the Agency, O&M Status Reports will contain at a minimum the contents outlined in Attachment J, Minimum Content for Project and O&M Deliverables.
-





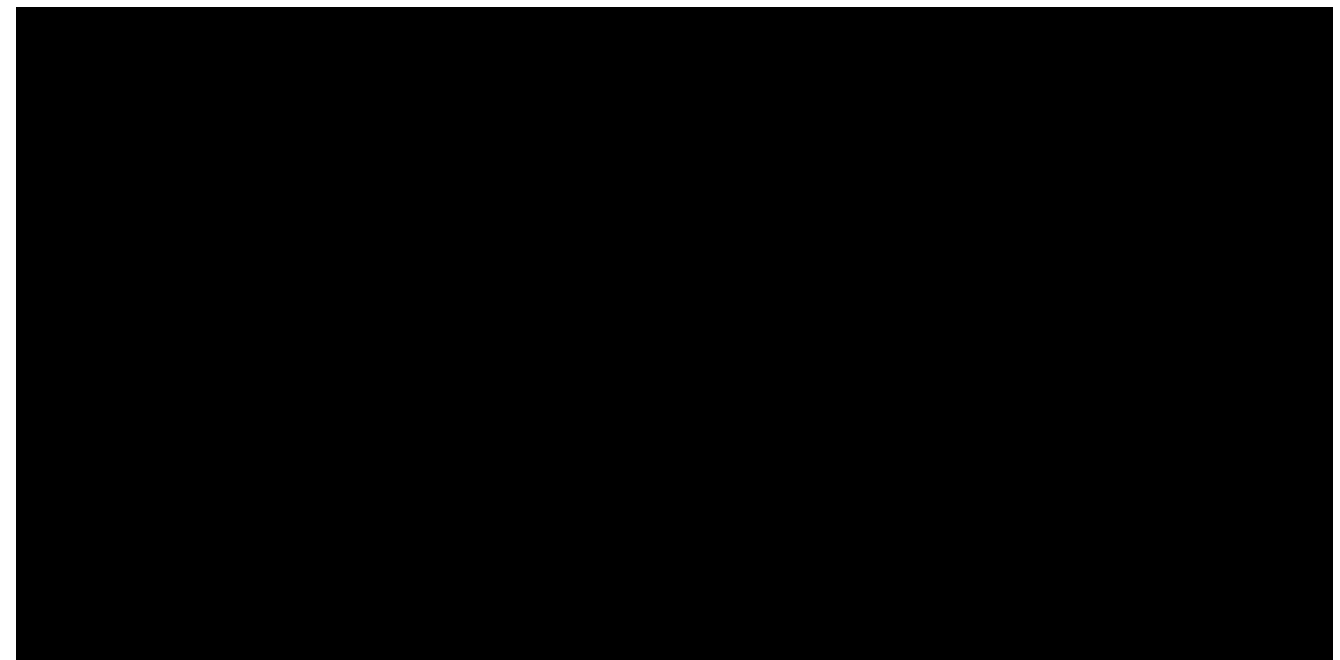


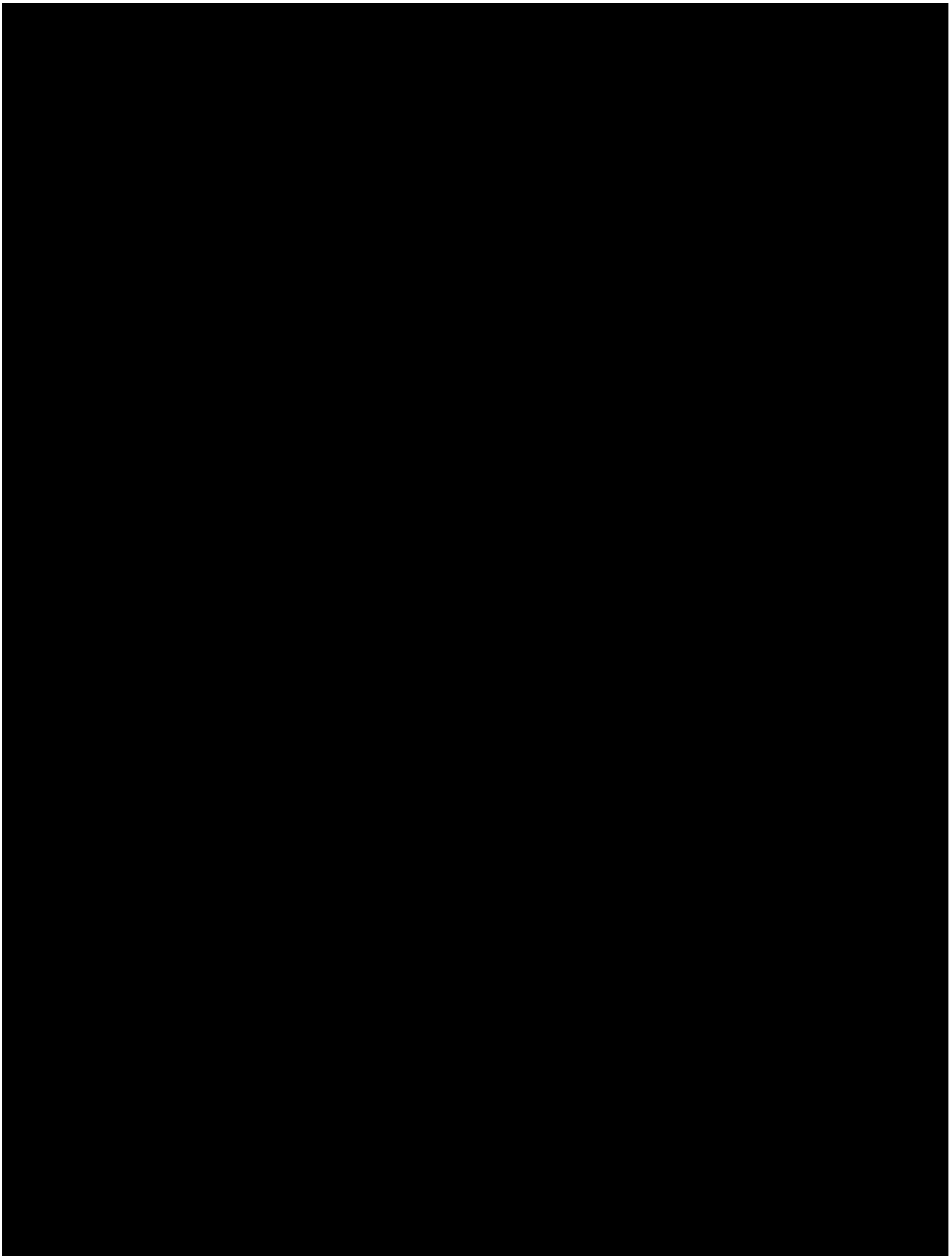


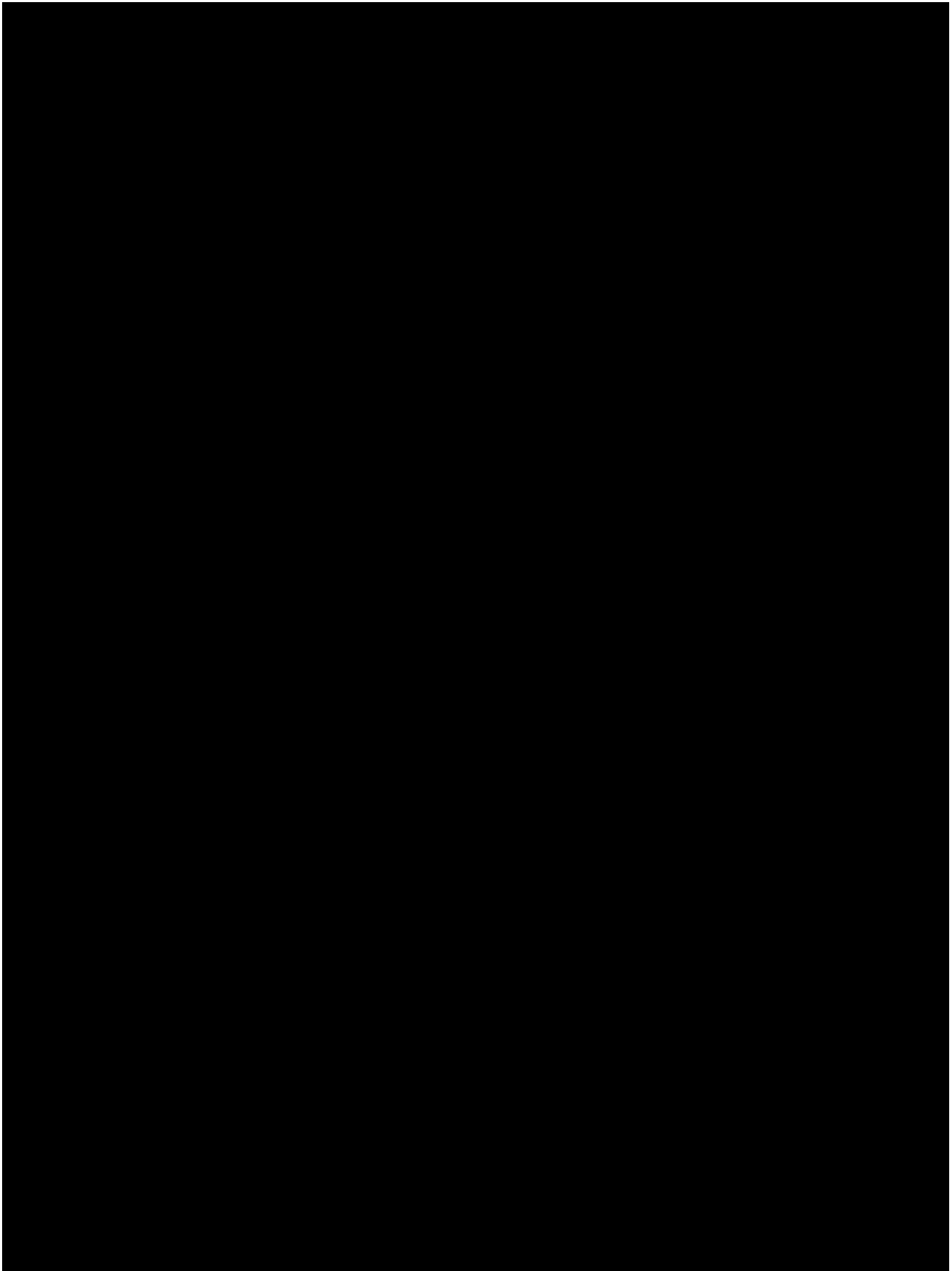


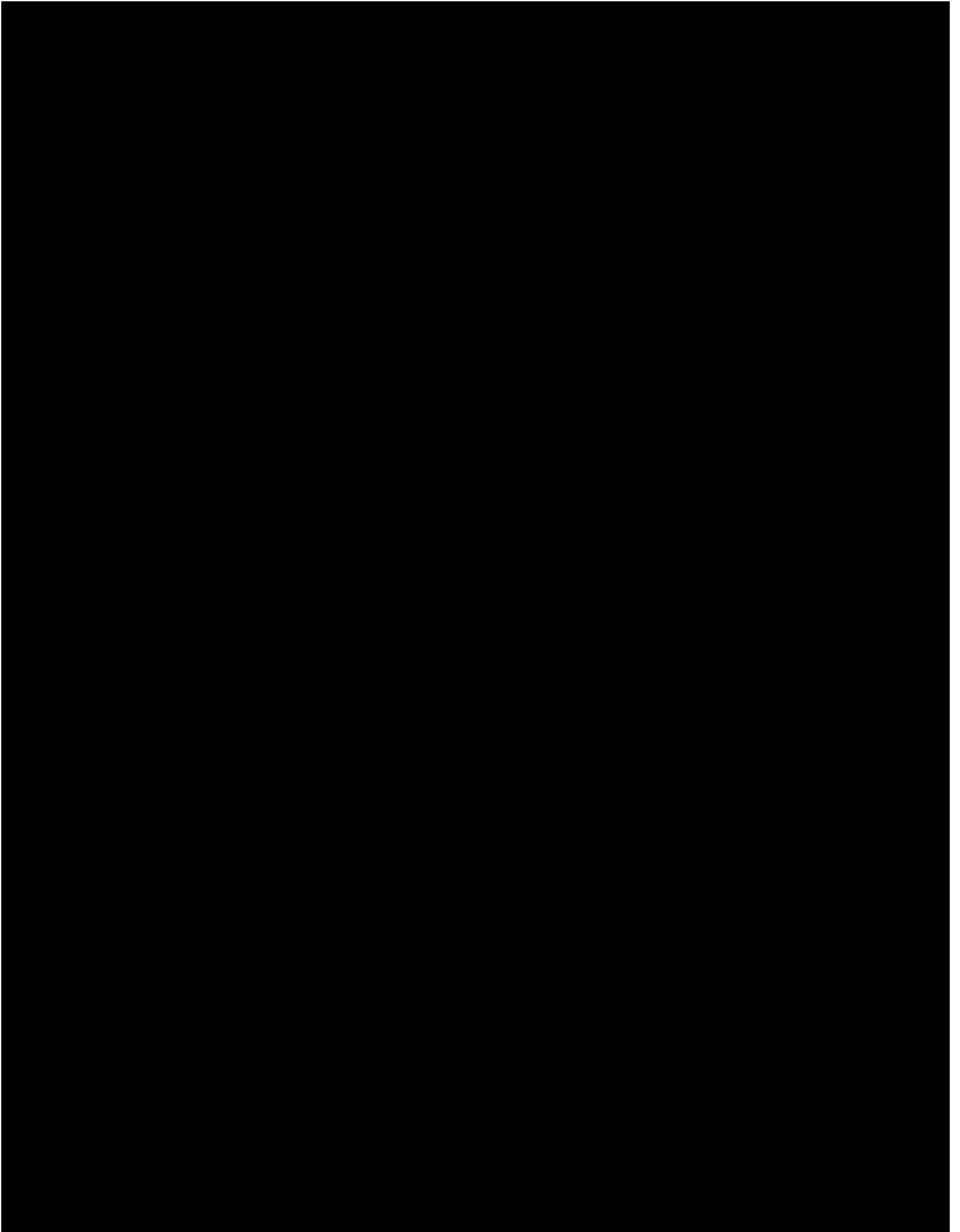
2. Vendor Hosting

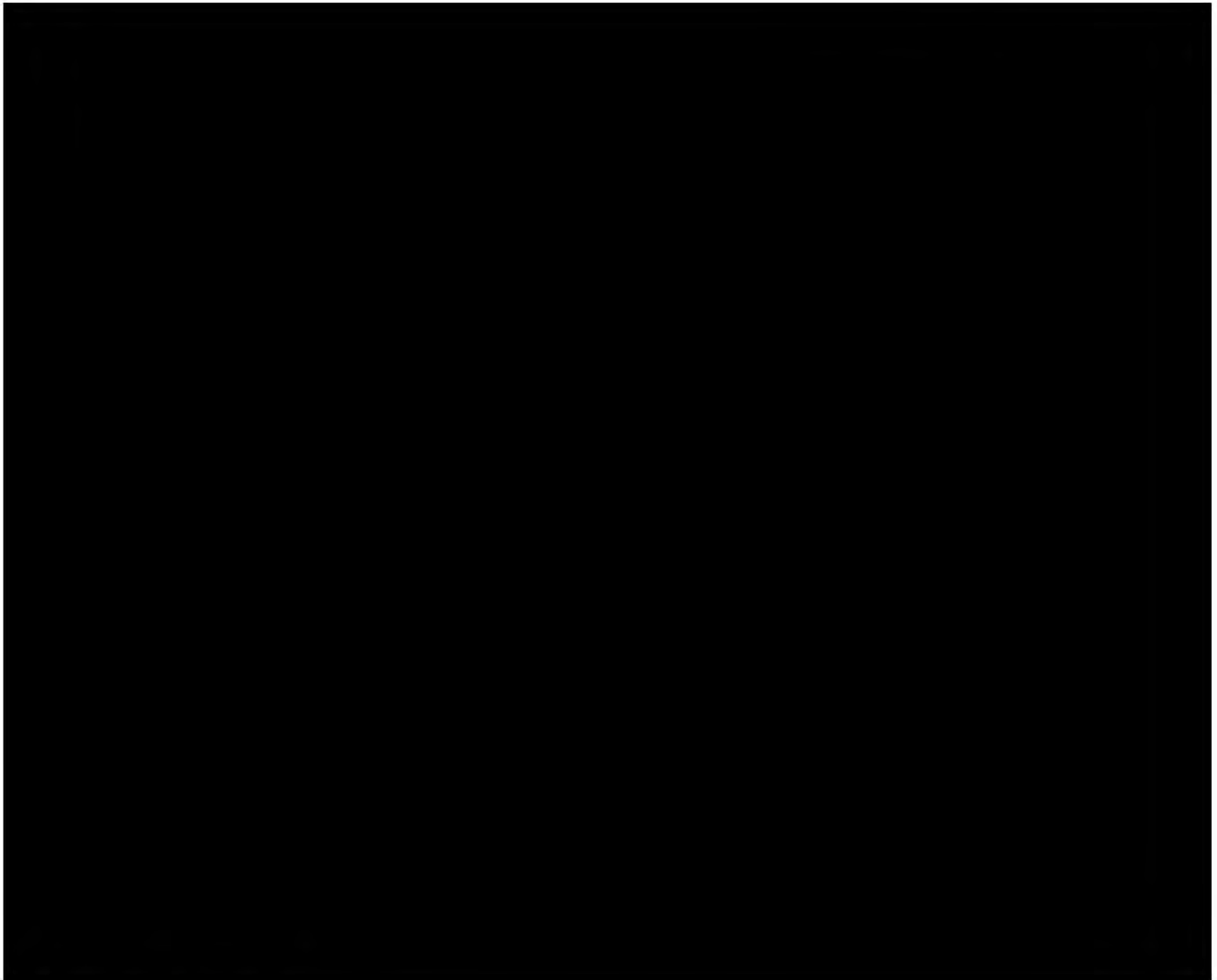
a. Describe your development, test, training, production, disaster recovery, and any separate reporting technical hosting environments.











3. State Hosting

- a. Describe the development, test, training, production, disaster recovery, and any separate reporting technical hosting environments the State will need to establish and operate to host the Solution.
 - b. Describe the schedule required to stand up each technical hosting environment.
 - c. Describe how the Vendor will assist the State to troubleshoot, review, maintain and upgrade all technical environments (servers, operating systems, utility software application software, and SAN storage) as needed to ensure continual compliance/conformance (as applicable) with federal, State, and DHHS Architectural, privacy, and security policies and standards.
 - d. Indicate whether the Solution supports offline access and data entry if the WAN connection is not available.
 - e. Describe how you will support the State in performing disaster recovery tasks, including DR testing.
-

[Redacted] a [Redacted]

4. Metrics and Performance

- a. Describe how the proposed Solution ensures adequate space on servers, bandwidth, and response time in the Solution to allow for a minimum 690 concurrent users accessing, entering, and reporting information with a capacity to handle up to 1380 with minimal performance degradation.

b. Describe how the Solution provides capability for transaction response time to be consistent for all users directly interacting with the production environment, based on a common application access for network access point, processed and returned to the network access point:

- i. Ninety (90) percent of responses to occur in two (2) seconds or less.
- ii. Ninety-five (95) percent of responses: to occur in three (3) seconds or less.
- iii. Ninety-seven (97) percent of responses to occur in four (4) seconds or less.
- iv. Ninety-nine (99) percent of responses to occur in five (5) seconds or less.

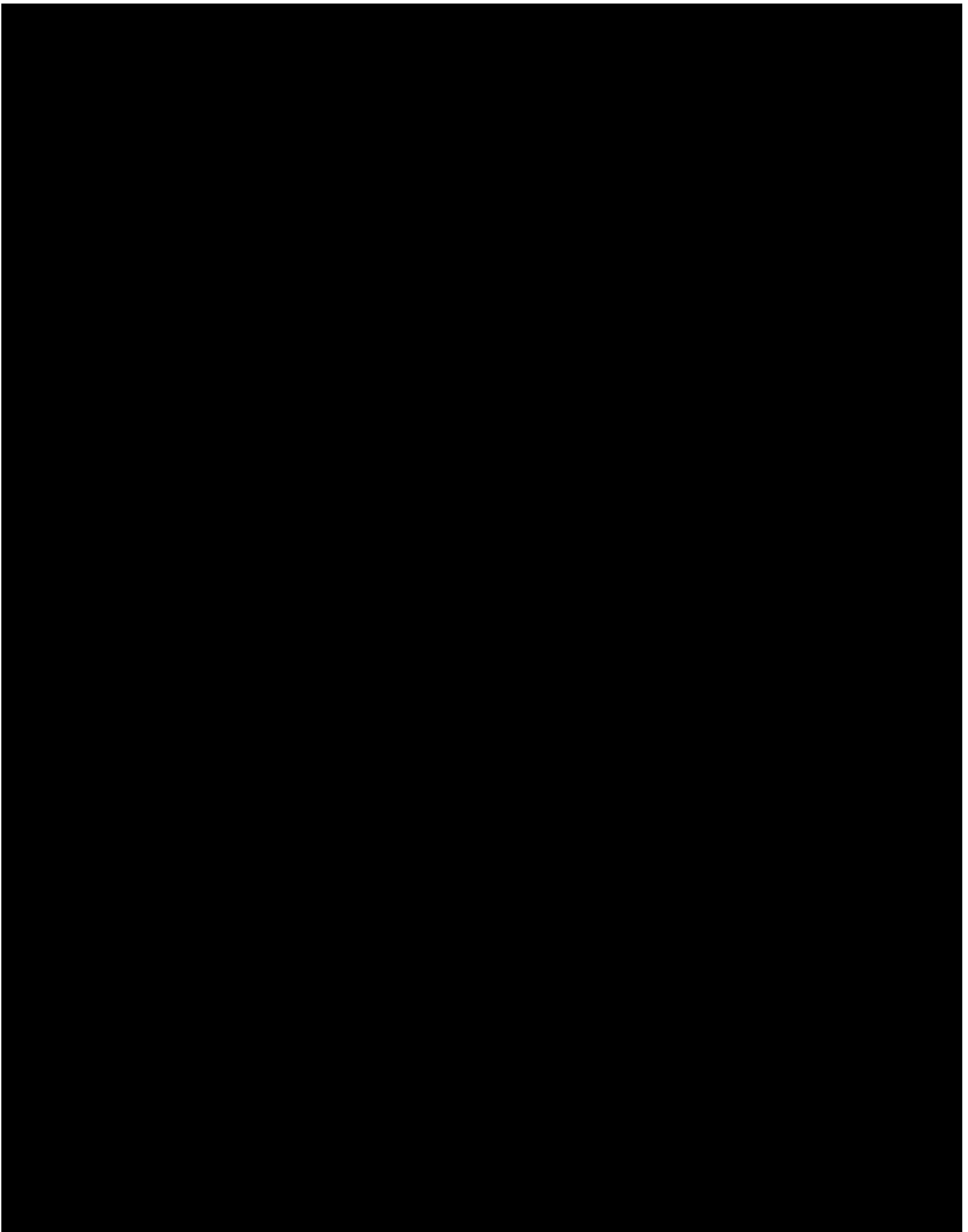
c. Describe your proposed Solution's established performance metrics, and whether it conforms to the response times listed above in b. of this specification. If a separate reporting environment is included in your proposal, please describe the response times for the environment.

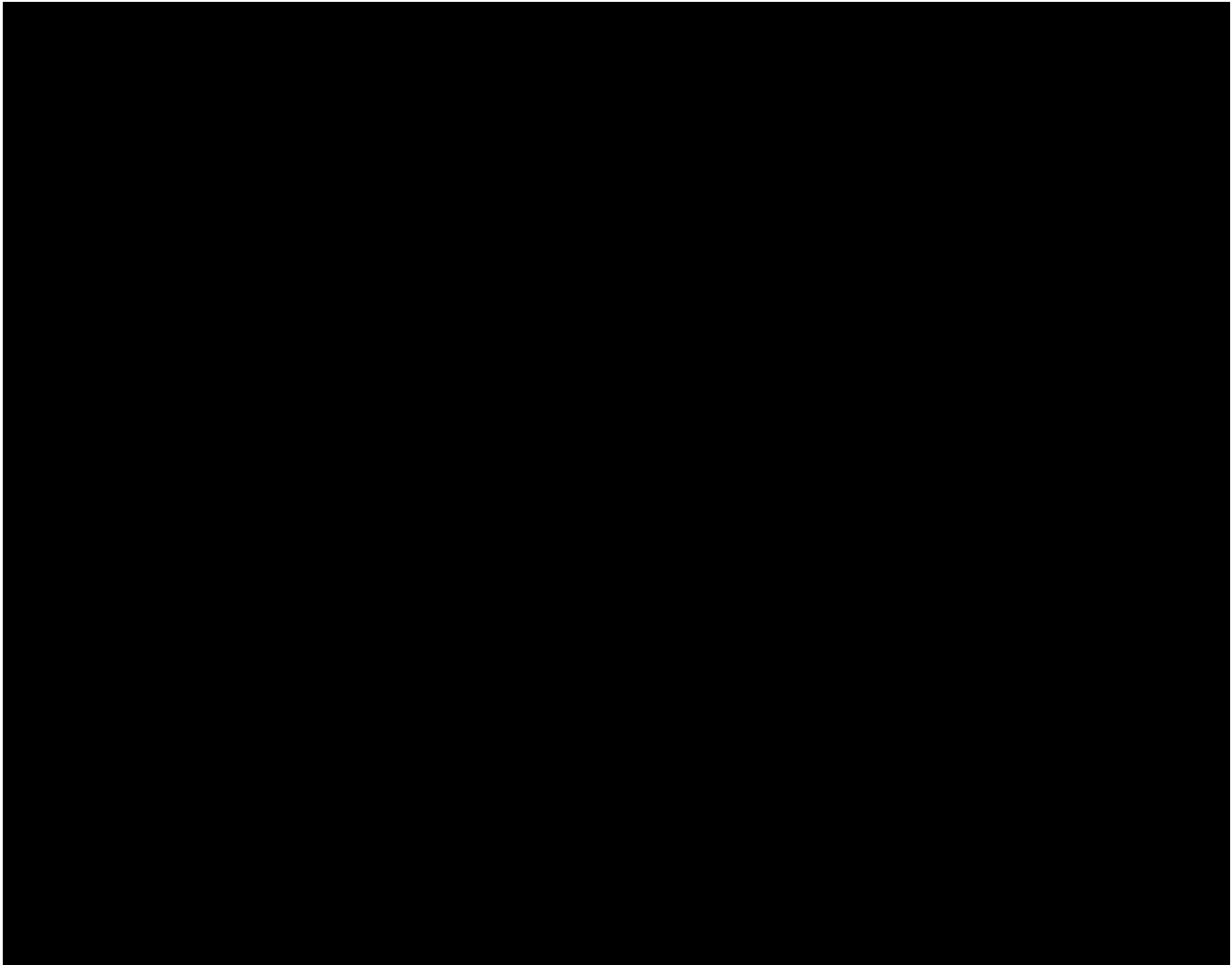
5. Vendor Service Level Agreement (SLA)

The Vendor will submit with its RFP response a draft SLA that defines formally the levels of service the Vendor will provide for the Solution during the Project and during O&M and addresses the Agency's service level expectations as listed below. Refer to Attachment J, Minimum Content for Project and O&M Deliverables for more information about the expectations of the SLAs contents.

The Agency's service level expectations for the Solution, its availability, and Vendor services are as follows:

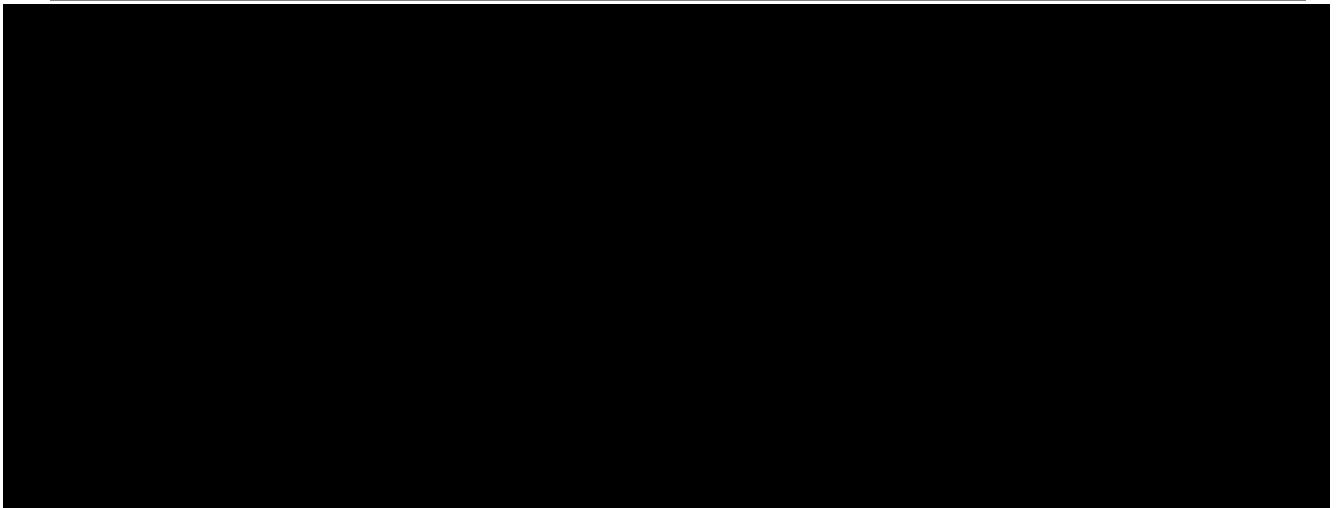
- a. Provide 99.9%, 24x7x365 system availability for all calendar days except for any system maintenance windows approved by the Agency.
 - b. Provide timely Solution upgrades for fixes and changes in the form of software releases and critical error fixes. Please discuss your support structure including, but not limited to, help desk, problem tracking, maintenance windows and hours of operation.
-

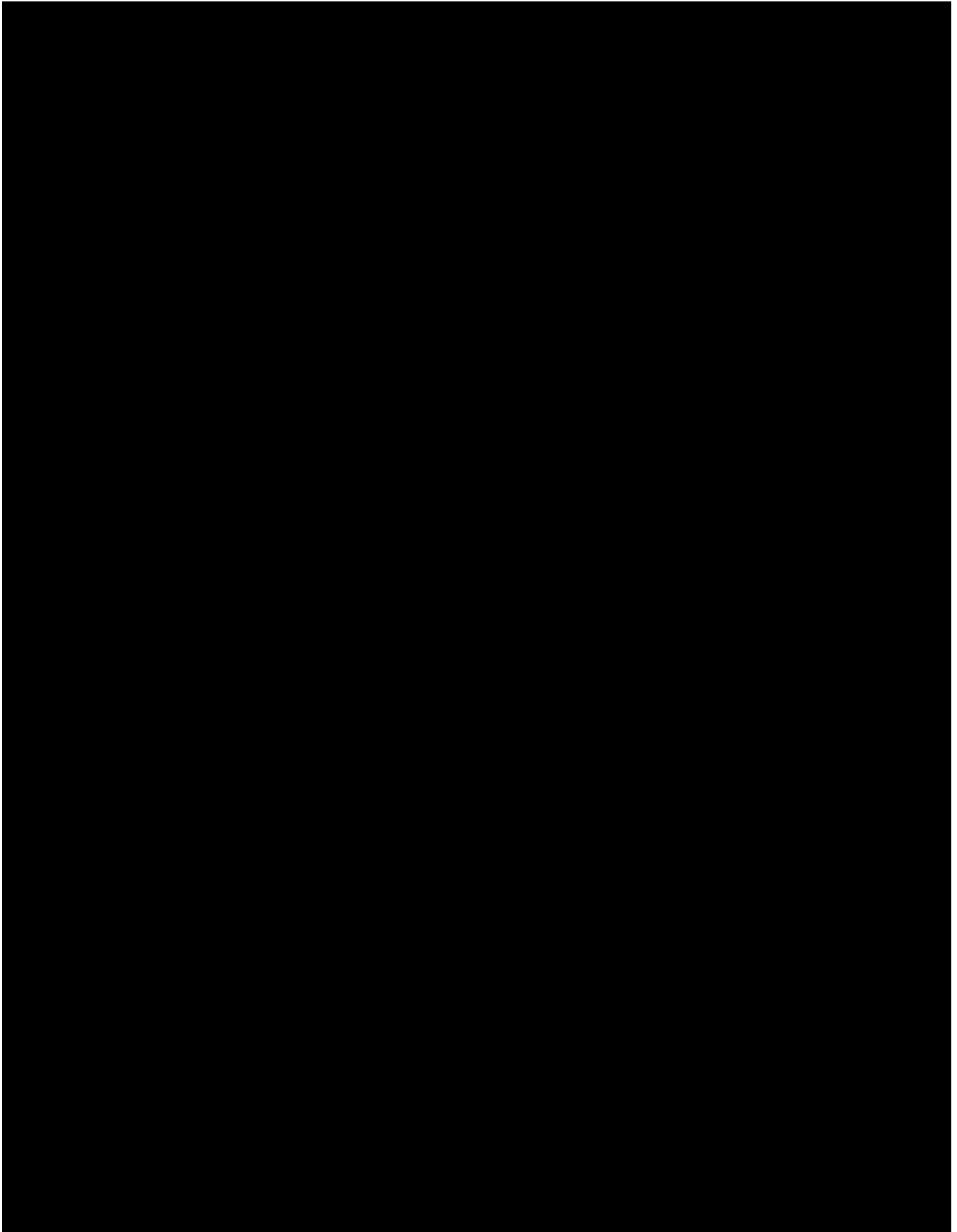


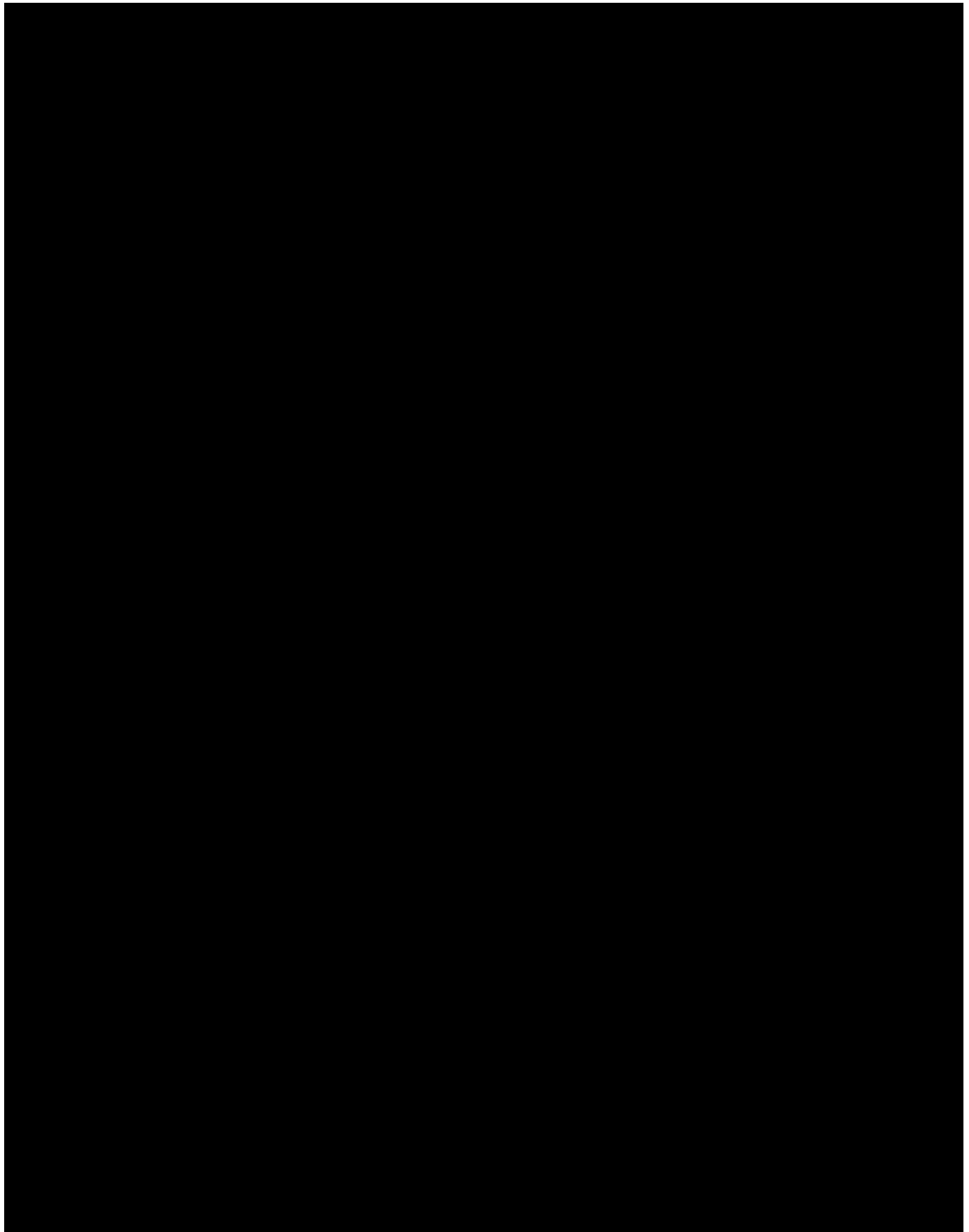


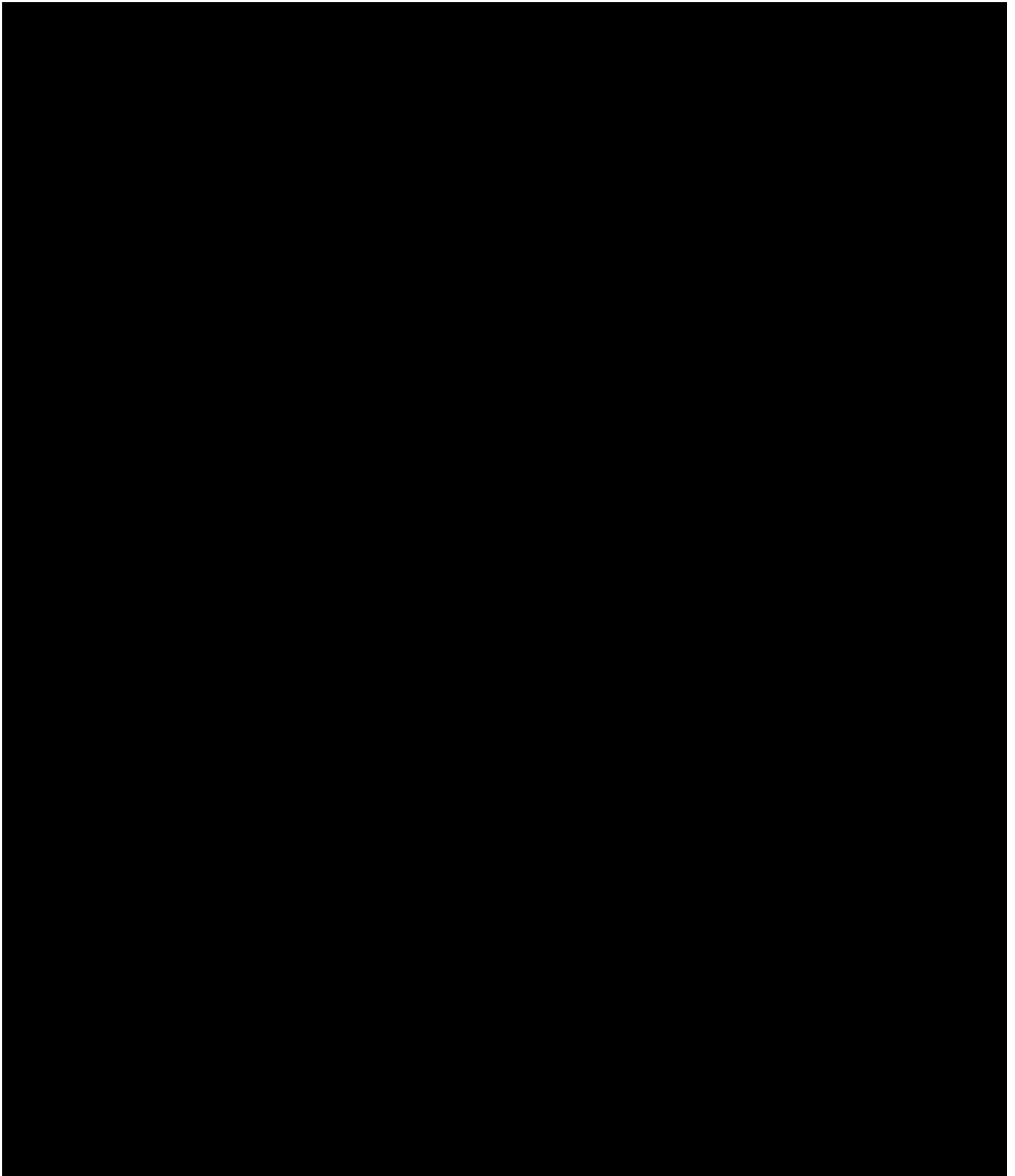
6. Help Desk Support

- a. Describe the help desk support you provide and indicate whether the support is available Monday through Friday 7:00 a.m. – 6:00 p.m. ET. Help desk support activity is considered resolution of the following:
- i. Category 1, 2, or 3 problems;
 - ii. Persistent product instability;
 - iii. Application of advanced tools for intensive research and development to produce a new release to fix the issue reported;
 - iv. Auditing ability unavailable; and
 - v. Escalated application errors.
-



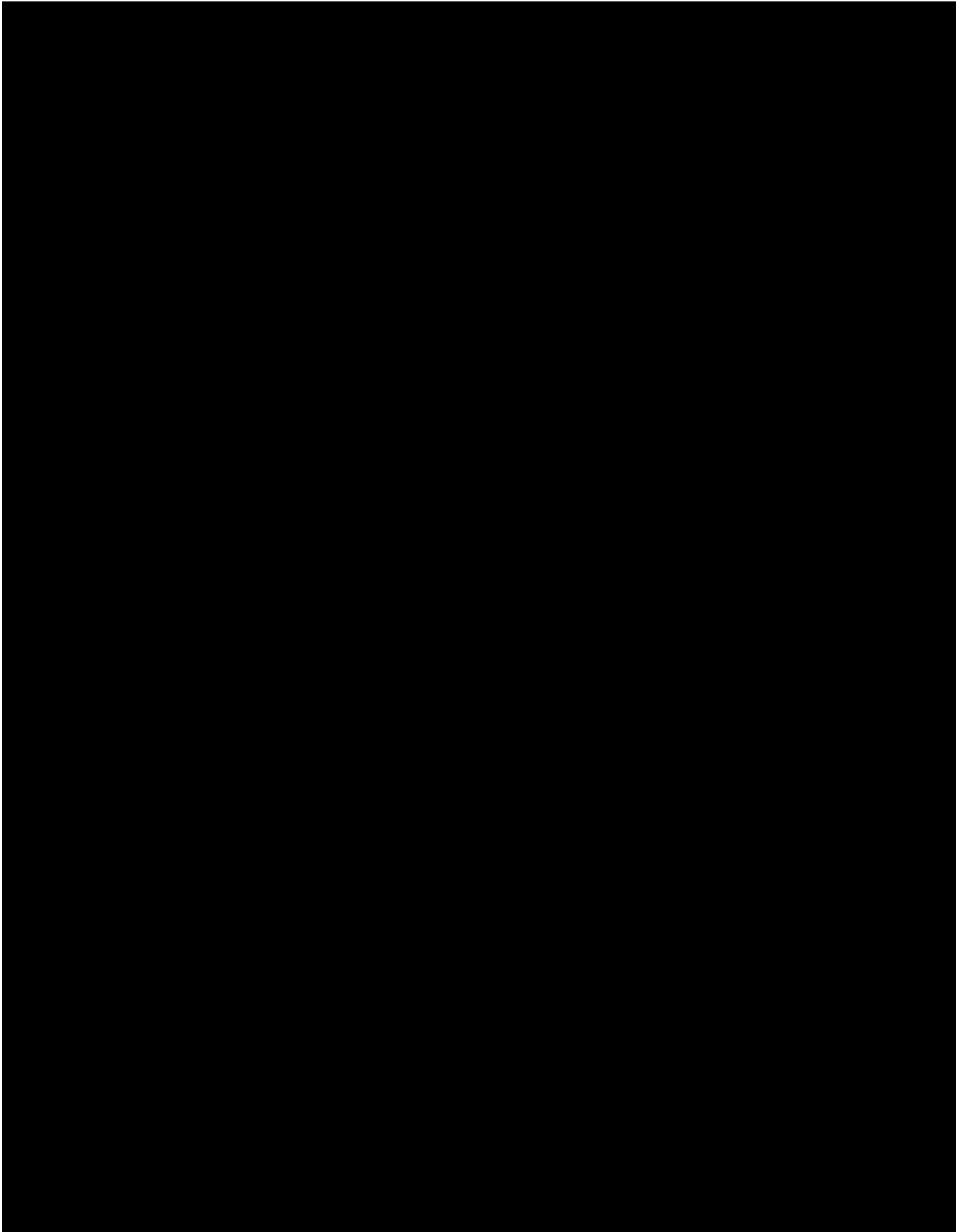


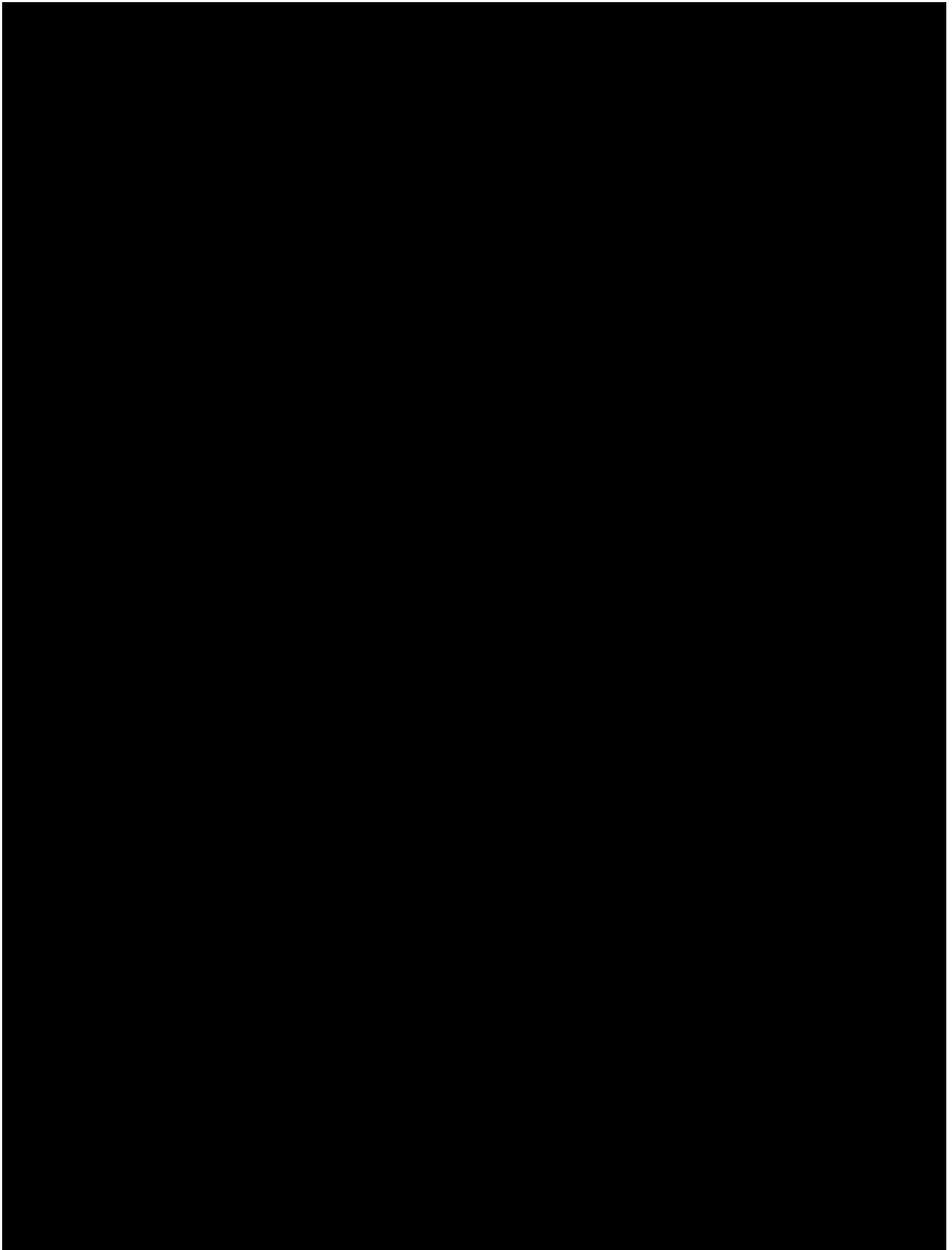


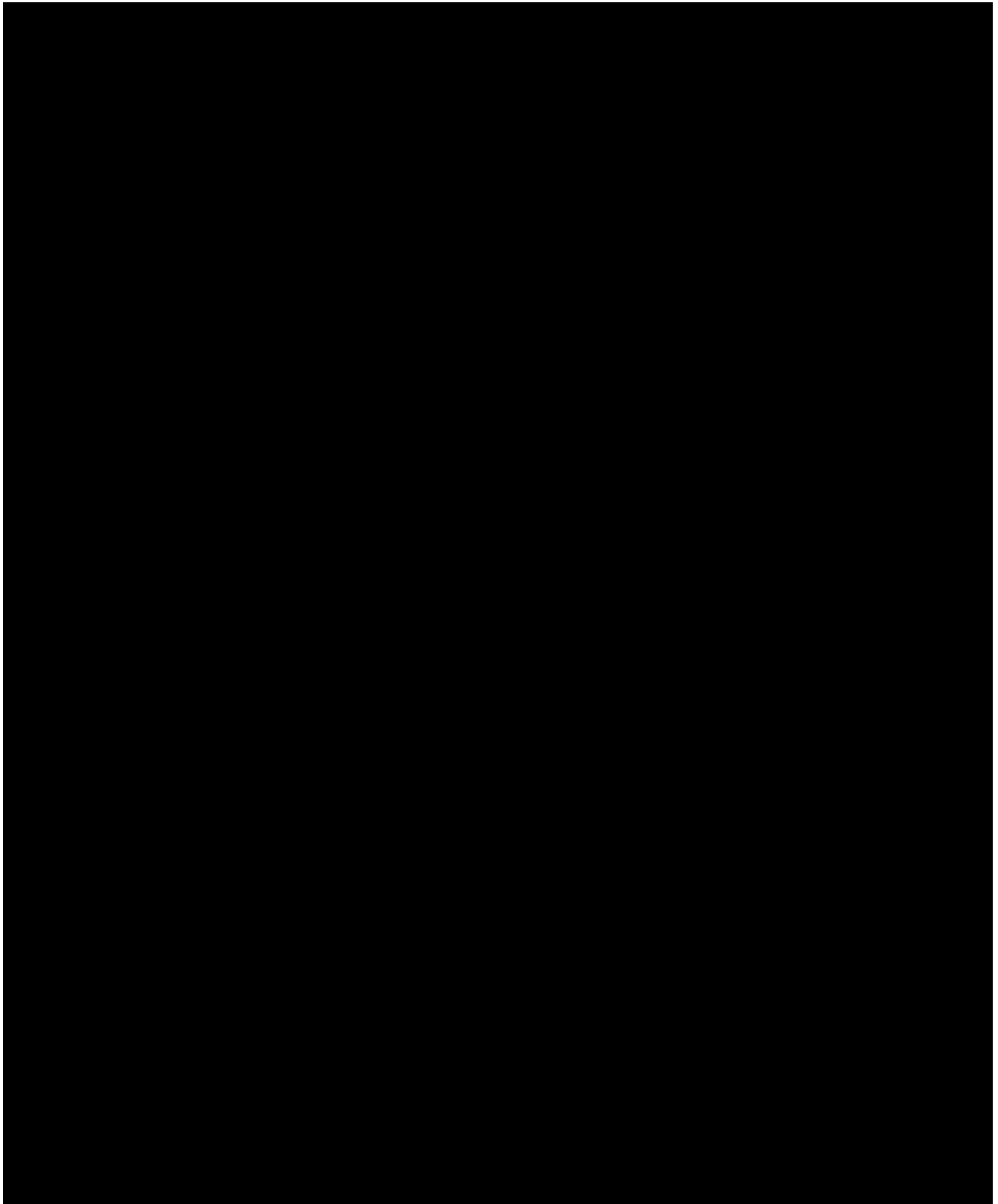


7. Acquisition, Licensing, and Product Overview

a. Describe all licensing options and licenses terms for your software, including Third-Party software if used as part of your Solution. The Third-Party Software License Agreements are to be included in the Vendor's offer.







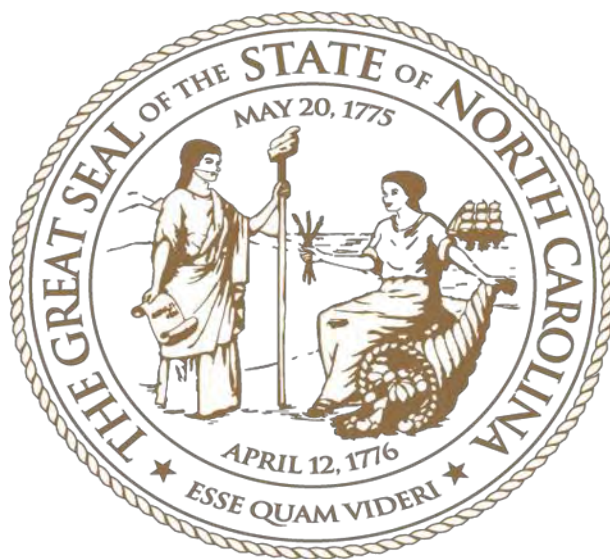


Section e)

Security Vendor Readiness Assessment Report (VRAR)

e) Security Vendor Readiness Assessment Report (VRAR)

ENTERPRISE SECURITY & RISK MANAGEMENT OFFICE (ESRMO)



Vendor Readiness Assessment Report (VRAR) for Solutions Not Hosted on State Infrastructure

● Executive Summary

The State of NC requires that all systems connected to the State Network or process State data, meet an acceptable level of security compliance. This includes those systems that operate outside of the States' direct control such as Cloud Services defined as Software as a Service (SaaS), Infrastructure as a Service (IaaS) or Platform as a Service (PaaS).

The State of NC has adopted the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 as the foundation for identifying and implementing information technology security controls. These controls are described in the State of NC Statewide Information Security Manual (SISM).

The following is a high-level view of specific security requirements that are needed to meet compliance. The control references (e.g., AC-2) refer to the specific NIST 800-53 control as listed in the SISM, which may be found at the following link: <https://it.nc.gov/statewide-information-security-policies>.

Note: There may be additional requirements depending on the sensitivity of the data and other Federal and State mandates, or agency specific requirements.

Table of Contents

Executive Summary	i
1. Introduction	1
1.1. Purpose	1
1.2. Outcomes	1
1.3. State Approach and Use of This Document	1
2. VENDOR System Information	2
2.1. Relationship to Other Vendors or CSPs	2
2.2. Data Flow Diagrams	3
2.3. Separation Measures [AC-4, SC-2, SC-7]	3
2.4. System Interconnections	3
3. Capability Readiness	4
3.1. State Mandates	4
3.2. State Requirements	5
3.2.1. Data at Rest and Authentication [SC-13]	5
3.2.2. Transport Layer Security [NIST SP 800-52, Revision 2]	5
3.2.3. Identification and Authentication, Authorization, and Access Control	6
3.2.4. Audit, Alerting, Malware, and Incident Response	7
3.2.5. Contingency Planning and Disaster Recovery	8
3.2.6. Configuration and Risk Management	8
3.2.7. Data Center Security	10
3.2.8. Policies, Procedures, and Training	10
3.3. Additional Capability Information	13
3.3.1. Staffing Levels	13
3.3.2. Change Management Maturity	13
3.3.3. Vendor Dependencies and Agreements	13
3.3.4. Continuous Monitoring Capabilities	14
3.3.5. Status of System Security Plan (SSP)	15

List of Tables

Table 2-1. System Information	2
Table 2-2. Leveraged Systems	2
Table 2-3. Leveraged Services	2
Table 2-4. System Interconnections	3
Table 2-5. Interconnection Security Agreements (ISAs)	3
Table 3-1. State Mandates	4
Table 3-2a. Data at Rest & Authentication	5
Table 3-2b. Transport Encryption	5
Table 3-3. Transport Protocol	5
Table 3-4. Identification and Authentication, Authorization, and Access Control	6
Table 3-5. Audit, Alerting, Malware, and Incident Response	7
Table 3-6. Contingency Planning and Disaster Recovery	8
Table 3-7. Configuration and Risk Management	8
Table 3-8. Data Center Security	10
Table 3-9. Policies and Procedures	10
Table 3-10. Missing Policy and Procedure Elements	12
Table 3-11. Security Awareness Training	12
Table 3-12. Staffing Levels	13
Table 3-13. Change Management	13
Table 3-14. Vendor Dependencies and Agreements	13
Table 3-15. Vendor Dependency Details	14
Table 3-16. Formal Agreements Details	14
Table 3-17. Continuous Monitoring Capabilities	14
Table 3-18. Continuous Monitoring Capabilities – Additional Details	14
Table 3-19. Maturity of the System Security Plan	15
Table 3-20. Controls Designated “Not Applicable”	15
Table 3-21. Controls with an Alternative Implementation	15

1. Introduction

1.1. Purpose

This report and its underlying assessment are intended to enable State agencies to reach a state-ready decision for a specific system **not hosted** on the State of NC's infrastructure that is based on organizational processes and the security capabilities of the Moderate/Low-impact information system.

1.2. Outcomes

Submission of this report by the Vendor **does not guarantee** a state-ready designation, nor does it guarantee that the State will procure services from the vendor.

1.3. State Approach and Use of This Document

The VRAR identifies clear and objective security capability requirements, where possible, while also allowing for the presentation of more subjective information. The clear and objective requirements enable the vendor to concisely identify whether an application or vendor is achieving the most important State Moderate or Low baseline requirements. The combination of objective requirements and subjective information enables State to render a readiness decision based on a more complete understanding of the vendor's security capabilities.

Section 4, Capability Readiness, is organized into three sections:

- **Section 3.1, State Mandates**, identifies a small set of the state mandates a vendor must satisfy. State **will not** waive any of these requirements.
- **Section 3.2, State Requirements**, identifies an excerpt of the most compelling requirements from the National Institute of Science and Technology (NIST) Special Publication (SP) 800 document series and State guidance. A VENDOR is unlikely to achieve approval if any of these requirements are not met.
- **Section 3.3, Additional Capability Information**, identifies additional information that is not tied to specific requirements, yet has typically reflected strongly on a VENDOR's ability to achieve approval.

2. **VENDOR System Information**

Provide and validate the information below. For example, if the deployment model is Government only, ensure there are no non-Government customers. The VRAR template is intended for systems categorized at the Moderate or Low security impact level, in accordance with the FIPS Publication 199 Security Categorization.

Table 2-1. System Information

<p>VENDOR Name: Salesforce</p> <p>System Name: Salesforce Platform</p> <p>Service Model: SaaS. Salesforce offers the market leading Platform as a Service (PaaS) and market leading Software as a Service (SaaS) solutions.</p> <p>FIPS PUB 199 System Security Level: On May 23, 2014, Salesforce achieved a FedRAMP Authority to Operate at the moderate impact level issued by the Department of Health and Human Services (HHS) for the Salesforce Government Cloud. Annually thereafter, HHS, as the FedRAMP authorizing agency, has approved the Salesforce Government Cloud authorization package that is updated based on annual attestation requirements and updates to the FedRAMP baseline which is FISMA compliant and based on the current release of NIST SP 800-53 Rev. 4. NIST 800-53 incorporates FIPS 199 and 200 standards.</p> <p>Fully Operational as of: Salesforce introduced its first service in February 2000.</p> <p>Number of Customers (State/Others): Salesforce has over 150,000 customers, across nearly every industry worldwide and which encompass all sizes of customers from less than 1,000 employees to greater than 50,000 employees. This includes our government customers representing 1,000 government agencies, 15 out of 15 federal cabinet level agencies, and most of the United States. Salesforce does not publicly disclose the breakdown of total number of customers using Salesforce for specific use cases, by vertical, geography, or total number of customers or end users using each specific Salesforce product.</p> <p>Deployment Model: Salesforce’s deployment model is a Community Cloud infrastructure, as defined by NIST SP 800-145. In the Salesforce Government Cloud, an organization dynamically provisions computing resources over the Internet on our multi-tenant infrastructure. This is a cost-effective deployment model for organizations as it gives them the flexibility to procure only the computing resources they need and delivers all services with consistent availability, resiliency, security, and manageability. The Salesforce Government Cloud is a dedicated instance of Salesforce’s multi-tenant Community Cloud infrastructure, specifically for use by U.S. federal, state, and local government customers, U.S. government contractors, and Federally Funded Research and Development Centers (FFRDCs). The isolated Production infrastructure supporting the Salesforce Government Cloud Customer Data ensures that the physical hardware in Salesforce’s colocation data centers that process, store, and transmit unencrypted Government Customer data are separate from hardware supporting other customers. While isolated, the underlying infrastructure supporting the Salesforce Government Cloud is the same trusted architecture model that supports Salesforce’s multi-tenant public cloud offering and over 5 billion customer transactions a day.</p> <p>System Functionality: Salesforce provides a single enterprise platform that delivers multiple services and enables the State to rapidly configure solutions specifically tailored to your mission and</p>

requirements. Salesforce solutions free data from legacy systems, empower customers, and connect organizations, and employees to administer services in powerful new ways. The Salesforce Platform is the lowest risk and fastest way to securely build, connect, optimize, and deploy every kind of app tailored for any type of use case.

2.1. Relationship to Other Vendors or CSPs

If this system resides in another VENDOR’s environment or inherits security capabilities, please provide the relevant details in Tables 2-2 and 2-3 below. **Please note**, the leveraged system itself must be State Authorized. For example, a large VENDOR may have a commercial service offering and a separate service offering with a State Authorization. Only the service offering with the State Authorization may be leveraged.

IMPORTANT: If there is a leveraged system, be sure to note below every capability that partially or fully leverages the underlying system. When doing so, indicate the capability is fully inherited or describe both the inherited and non-inherited aspects of the capability.

List all **services** leveraged. The system from which the service is leveraged must be listed in Table 2-2 above.

Table 2-3. Leveraged Services

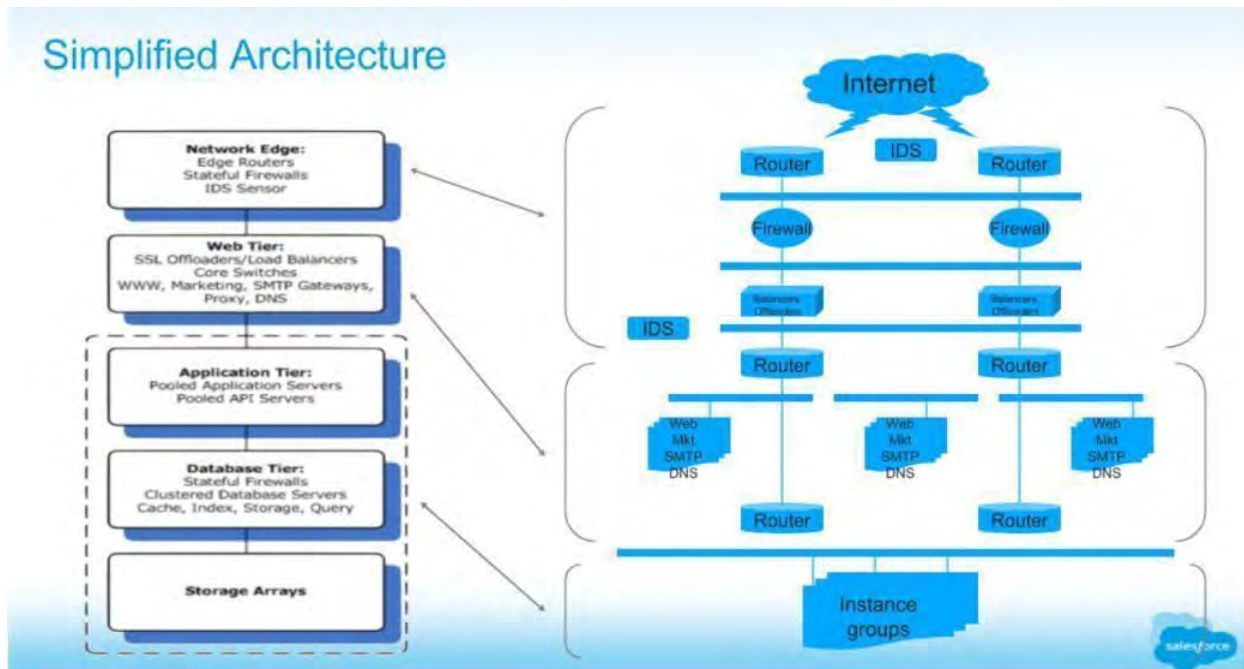
#	Service	Service Capability	System
---	---------	--------------------	--------

		<p>Compliance Program (https://marketplace.fedramp.gov/#/product/aws-govcloud?sort=productName&productNameSearch=AWS). Data centers are monitored using AWS global Security Operations Centers, which are responsible for monitoring, triaging, and executing security programs. They provide 24/7 global support by managing and monitoring data center access activities, equipping local teams and other support teams to respond to security incidents by triaging, consulting, analyzing, and dispatching responses. Physical access points to server rooms are recorded by Closed Circuit Television Camera (CCTV). Images are retained according to legal and compliance requirements. Physical access is controlled at building ingress points by professional security staff utilizing surveillance, detection systems, and other electronic means. Authorized staff utilize multi-factor authentication mechanisms to access data centers. Entrances to server rooms are secured with devices that sound alarms to initiate an incident response if the door is forced or held open.</p>	
--	--	--	--

2.2. Data Flow Diagrams

Insert Vendor-validated data flow diagram(s) and provide a written description of the data flows. The diagram(s) must:

- clearly identify anywhere State data is to be processed, stored, or transmitted;
- clearly delineate how data comes into and out of the system boundary;
- clearly identify data flows for privileged, non-privileged and customer access; and
- depict how **all ports, protocols, and services** of all inbound and outbound traffic are represented and managed.



The Salesforce instance where state data will be processed, stored, or transmitted will be hosted on Government Cloud Plus within continental US with services performed in isolated infrastructure by qualified US citizens. All data to and from the Salesforce instance is encrypted in transit via HTTPS. All users irrespective of privilege log securely into Salesforce over HTTPS. For all inbound and outbound traffic all data will flow over port 443 using the HTTPS protocol for transport with REST/SOAP/SAML and any other protocols layered on top. All web services will use either the REST or SOAP API.

2.3. Separation Measures [AC-4, SC-2, SC-7]

Assess and describe the strength of the physical and/or logical separation measures in place to provide segmentation and isolation of tenants, administration, and operations; addressing user-to-system; admin-to-system; and system-to-system relationships.

The Vendor must base the assessment of separation measures on very strong evidence, such as the review of any existing penetration testing results, or an expert review of the products, architecture, and configurations involved. The Vendor must describe how the methods used to verify the strength of separation measures.

Salesforce services its customers using what is known in the industry as “multi-tenant” architecture. Multi-tenant applications and platforms permit many users to simultaneously access and use the same services, with logical separation of data allowing each customer to view only its “instance” of Salesforce’s services and associated data. Salesforce’s multi-tenant architecture is similar to that used to

provide online banking and brokerage services to consumers, which can also be accessed and used by thousands of users simultaneously through the logical – rather than physical – separation of data.

Salesforce's multitenant architecture and secure logical controls for the Salesforce Services address the separation of Customer Data. Salesforce does not use dedicated servers for a specific customer. The infrastructure for the Salesforce Services is divided into a modular architecture based on instance. Each instance can support several thousand customers in a secure and efficient manner.

A customer's instance (org) of Salesforce is an aggregate of the raw data. The data model is very complicated, normalized, and the rows are identified by base62 encoded keys (primary and foreign). Re-establishing data ownership and a business context for the data would be very difficult to do at the database level. To reassemble any given customer's application (org), someone would need access to our source code to reassemble the raw data in a manner that could be interpreted and understood and would need the entire set of tapes or disks/arrays supporting a given instance, as the data for any one customer is spread across several tapes/disks. Data center engineers with physical access to the servers do not have logical access to the production environment and administrators with logical access to the systems do not have physical access to the data centers.

2.4. System Interconnections

A System Interconnection is a dedicated connection between information systems, such as between a SaaS/PaaS and underlying IaaS.

The Vendor must complete the table below. If the answer to any question is "yes," please briefly describe the connection. Also, if the answer to the last question is "yes," please complete Table 2-5 below.

Table 2-4. System Interconnections

#	Question	Yes	No	If Yes, please describe.
1	Does the system connect to the Internet?	X		
2	Does the system connect to a corporate or state infrastructure/network?		X	
3	Does the system connect to external systems?		X	

If there are connections to external systems, please list each in the table below, using one row per interconnection. If there are no external system connections, please type "None" in the first row.

Table 2-5. Interconnection Security Agreements (ISAs)

#	External System Connection	Does an ISA Exist?		Interconnection Description. If no ISA, please justify below.
		Yes	No	
1	Not applicable.			
2	Not applicable.			

3. Capability Readiness

3.1. State Mandates

This section identifies State requirements applicable to all State approved systems. All requirements in this section must be met. Some of these topics are also covered in greater detail in Section 3.2, *State Requirements*, below.

Only answer "Yes" if the requirement is fully and strictly met. The Vendor must answer "No" if an alternative implementation is in place.

Table 3-1. State Mandates

#	Compliance Topic	Fully Compliant?	
		Yes	No
1	Data at Rest, Authentication: Are FIPS 140-2/-3 Validated or National Security Agency (NSA)-Approved cryptographic modules only used where cryptography is required?	X	
2	Transmission, Remote Access: Are FIPS 140-2/-3 Validated or National Security Agency (NSA)-Approved cryptographic modules consistently used where cryptography is required?	X	
3	Can the VENDOR'S solution integrate with the State's NCID solution?	X	
4	Does the VENDOR utilize security boundary/threat protection devices to protect the network, system, application...e.g., firewalls intrusion detection/prevention systems, end point protection etc.? [SC-7] [SI-3/SI-4]	X	
5	Does the VENDOR have the ability to consistently remediate High risk vulnerabilities within 30 days and Medium risk vulnerabilities within 60 days? [SI-2]	X	
6	Does the VENDOR and system meet Federal Records Management Requirements, including the ability to support record holds, National Archives and Records Administration (NARA) requirements, and Freedom of Information Act (FOIA) requirements?		X
7	Does the VENDOR store, process or transmit <u>State data</u> only in the continental US and is that data backed up in only US locations?	X	
8	Does the VENDOR have a process to securely dispose of State data from its systems upon request that is in accordance with the National Institute for Standards and Technology (NIST) Special Publication 800-88 revision 1 <u>and</u> will provide to the State a certificate of data destruction? [MP-6]	X	
9	All operating systems (OS) <u>AND</u> major application software components (e.g., Microsoft SQL, Apache Tomcat, Oracle Weblogic, etc.), must NOT be past N-1. Applications which are not operating on the most recent platform MUST have a roadmap to upgrade with a State approved timeline. Does the application support the N-1 requirement?	X	
10	Does the vendor have a current 3 rd party attestation certification <u>and</u> is it regularly renewed? The State requires an independent 3 rd party attestation (e.g., FedRAMP, SOC 2 Type 2, ISO 27001, or HITRUST) <i>prior to</i> contract award for systems containing Restricted/Highly Restricted data. Note: SaaS vendors cannot use IaaS/PaaS certification unless the application is explicitly covered as part of the IaaS/PaaS assessments. [CA-7, RA-3, SA-9]	X	

11	Does the VENDOR's staff have appropriate background checks for unprivileged and privileged access and accounts according to Federal and/or State designation procedures for those systems that require it? [AC-2, PS-3]	X	
----	---	---	--

3.2. State Requirements

This section identifies additional State Readiness requirements. All requirements in this section must be met; however, alternative implementations and non-applicability justifications may be considered on a limited basis.

3.2.1. Data at Rest and Authentication [SC-13]

The Vendor must ensure FIPS 140-2, or 140-3 where available, Validated or NSA-Approved algorithms are used for all encryption modules. FIPS 140-2 Compliant is not sufficient. The Vendor may add rows to the table if appropriate but must not remove the original rows. The Vendor must identify all non-compliant cryptographic modules in use.

Table 3-2a. Data at Rest & Authentication

	Cryptographic Module Type	FIPS 140-2 Validated?		NSA Approved?		Describe Any Alternative Implementations (if applicable)	Describe Missing Elements or N/A Justification
		Yes	No	Yes	No		
1	Data at Rest [SC-28]	X					
2	Authentication [IA-5, IA-7]	X					

3.2.2. Transport Layer Security [NIST SP 800-52, Revision 2]

The Vendor must ensure FIPS 140-2, or 140-3 where available, Validated or NSA-Approved algorithms are used for all encryption modules relating to block ciphers, digital signatures and hash functions. Full FIPS mode is not required unless other regulatory requirements must be met. The Vendor may add rows to the table if appropriate but must not remove the original rows. The Vendor must identify all non-compliant cryptographic modules in use.

Table 3-2b. Transport Encryption

	Cryptographic Module Type	FIPS 140-2 Validated?		NSA Approved?		Describe Any Alternative Implementations (if applicable)	Describe Missing Elements or N/A Justification
		Yes	No	Yes	No		
1	Transmission [SC-8 (1), SC-12, SC-12 (2, 3)]	X					
2	Remote Access [AC-17 (2)]	X					

The Vendor must identify all protocols in use. The Vendor may add rows to the table if appropriate, but must not remove the original rows.

Table 3-3. Transport Protocol

#	The Cryptographic Module Type	Protocol In Use?		If "yes," please describe use for both internal and external communications
		Yes	No	

1	SSL (Non-Compliant)	X		All transmissions between the user and the Salesforce Services are secured using TLS 1.2 and encrypted using 256 or 128-bit key. The Services use International/Global Set Up SSL certificates with 2048-bit Public Keys.
2	TLS 1.0 (Non-Compliant)		X	
3	TLS 1.1 (Non-Compliant)		X	
4	TLS 1.2 (Compliant)	X		All transmissions between the user and the Salesforce Services are secured using TLS 1.2 and encrypted using 256 or 128-bit key. The Services use International/Global Set Up SSL certificates with 2048-bit Public Keys.
5	TLS 1.3 (Compliant)		X	

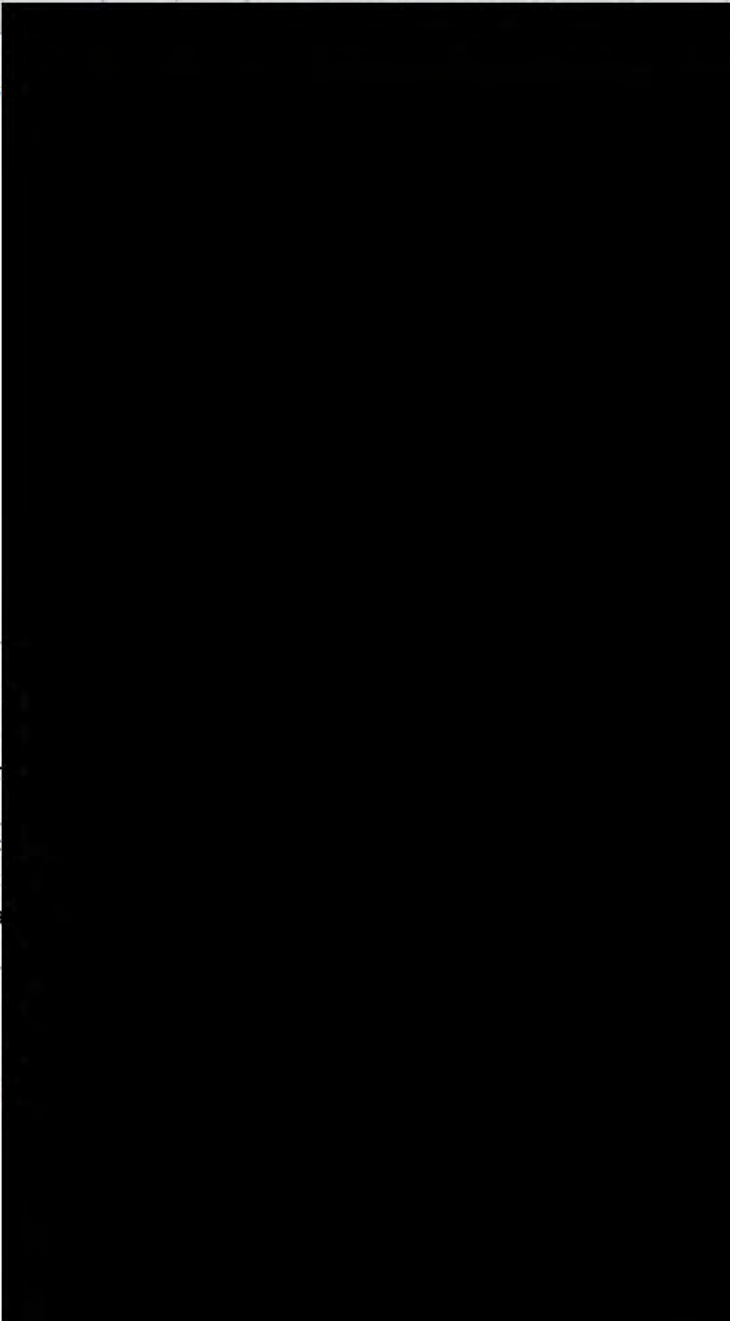
3.2.3. Identification and Authentication, Authorization, and Access Control

Only answer “yes” if the answer is consistently “yes.” For partially implemented areas, answer “no” and describe what is missing to achieve a “yes” answer. If inherited, please indicate partial or full inheritance in the “Describe Capability” column. Any non-inherited capabilities must be described.

Table 3-4. Identification and Authentication, Authorization, and Access Control

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
1	Does the system uniquely identify and authorize organizational users (or processes acting on behalf of organizational users) in a manner that cannot be repudiated, and which sufficiently reduces the risk of impersonation? [IA-2, IA-4]	X		
2	Does the system require multi-factor authentication (MFA) for administrative accounts and functions? [IA-2, IA-2 (1), IA-2 (2)]	X		
3	Is role-based access used, managed, and monitored? [IA-4, IA-5]	X		
4	Does the system restrict non-authorized personnel’s access to resources? [AC-6, AC-6 (1), AC-6 (2)]	X		
5	Does the system restrict non-privileged users from performing privileged function? [AC-6, AC-6 (1), AC-6 (2), AC-6 (10)]	X		

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
6	Does the system ensure secure separation of customer data? [SC-4]			

#	Question	Describe capability, supporting
7	Does the system ensure secure separation of customer processing environments [2]	
8	Does the system restrict access of administrative personnel in a way that the capability of individuals to compromise the security of the information system [2]	
9	Does the remote access capability include VENDOR-defined and implemented user restrictions, configuration guidance, and authorization procedure? [AC-17]	
10	How will the State's password policy be enforced? State requires minimum 12 character complex passwords (Upper/Lower, Special Character & Numerical)	

3.2.4. Audit, Alerting, Malware, and Incident Response

Only answer “yes” if the answer is consistently “yes.” For partially implemented areas, answer “no” and describe what is missing to achieve a “yes” answer. If inherited, please indicate partial or full inheritance in the “Describe Capability” column. Any non-inherited capabilities must be described.

Table 3-5. Audit, Alerting, Malware, and Incident Response

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
---	----------	-----	----	--

1	Does the system have the capability to detect, contain, and eradicate malicious software? [SI-3]	X	<p>Salesforce's Computer Security Incident Response Team (CSIRT) uses a security event logging and management system to manage the security alerts and logs generated by devices on our network. The system consists of a central database, management server, and distributed agents. The distributed agents receive events from network devices and systems (firewalls, IDS, routers, switches, hosts, file integrity, and database monitoring) on the network, then compress, encrypt, and transmit the data to the management server and database for processing. Correlated events are configured to generate alerts and logs which are monitored on a 24/7 basis. Firewalls and IDS systems are configured with automated syslog notifications for key events.</p> <p>Controls have been implemented to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's commitments and system requirements as they relate to security, availability and confidentiality. Infrastructure is adequately protected with a variety of network security controls including but not limited firewall, routers, intrusion detection system with logging enabled and monitoring 24x7365 by the Salesforce Computer Security Incident Response Team (CSIRT).</p> <p>Servers have a vulnerability program, including anti-virus and regular patching. Regular vulnerability scans are performed in the environment. Anti-malware software is inherently included on Mac workstations and is installed on Windows employee laptops. Malware definition parent servers check for updates daily and push updates to end user</p>
---	--	---	---

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
				workstations, which are configured to prevent end-users from permanently disabling anti-malware scanning. Predefined configurations are reinforced upon next check-in for disabled clients. Privileged access to the managed anti-malware server, used to prevent and detect malicious software, is restricted to system administrators.

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
2	Does the system store audit data in a tamper-resistant manner which meets chain of custody and any e-discovery requirements? [AU-4, AU-9]	X		<p>Application auditing features include: - Record Modification Fields: All objects include fields to store the name of the user who created the record and who last modified the record. Login History: You can review a list of successful and failed login attempts to your organization for the past six months. Field History Tracking: You can also enable auditing for individual fields, which will automatically track any changes in the values of selected fields. Although auditing is available for all custom objects, only some standard objects allow field-level auditing. Setup Audit Trail: Administrators can also view a Setup Audit Trail, which logs when modifications are made to your organization's configuration. Detailed application logs can be used for forensics investigations by customers. These logs are stored for 12 months and are available for a fee. Shield include: - Event Monitoring: Event Monitoring enables customers to further investigate how their users are using the application. This includes insight into what Salesforce applications are being adopted by users' who is logging in and from where, what pages users are viewing, what reports users are running and exporting and other aspects of application usage. This is delivered as an API-first feature and there are Salesforce partners with visualization tools available. - Field Audit Trail: Field Audit Trail lets you define a policy to retain archived field history data up to ten years, independent of field history tracking. This feature helps you comply with industry regulations related to audit capability and data retention.</p>

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
3	Does the VENDOR have the capability to detect unauthorized or malicious use of the system, including insider threat and external intrusions? [SI-4, SI-4 (4), SI-4 (5), SI-7, SI-7 (7)]	X		Please refer to item #1.
4	Does the VENDOR log and monitor access to the system? [SI-4]	X		Please refer to item #1.
5	Does the VENDOR have an Incident Response Plan and a fully developed Incident Response test plan? [IR-3, IR-8]	X		<p>Salesforce has a formal Incident Management Process that guides the Salesforce Computer Security Incident Response team (CSIRT) in investigation, management, communication, and resolution activities. Salesforce will promptly notify the customer in the event of any security breach of the Services resulting in an actual or reasonably suspected unauthorized disclosure of customer data. Notification may include phone contact by Salesforce Support, email to the customer's administrator and Security Contact (if submitted by customer), and public posting on trust.salesforce.com. Regular updates are provided to engaged parties until issue resolution. Incident tracking and resolution is documented and managed within an internal ticketing system. If CSIRT requires additional assistance in responding to a complex, high severity incident, Salesforce can also exercise retainers that are in place with multiple external incident response consulting companies.</p>

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
6	Does the VENDOR have a plan and capability to perform security code analysis and assess code for security flaws, as well as identify, track, and remediate security flaws? [SA-11]	X		Salesforce provides training to its developers. The training covers the basics of application security - such as the OWASP Top 10. Additionally, in depth training and labs are available to employees. - Threat assessments are performed on all high-risk features during the design. These assessments help identify potential security issues early in the development process and help the QA team perform focused security testing during the release. Secure Coding - During development of features, developers utilize the valuable techniques identified during training to build security into their features. Secure coding patterns and anti-patterns exist that cover standard vulnerability types such as the OWASP Top 10 and CWE 25 have been written and are updated frequently to cover standard and sometimes obscure vulnerability types. Several static code analysis tools are run through the release process. Fortify, Checkmarx, FindBugs and several proprietary code analysis tools are used to identify security flaws as early in the development process as possible.
7	Does the VENDOR implement automated mechanisms for incident handling and reporting? [IR-4, IR-4 (1), IR-6]	X		Please refer to item #5.
8	Does the VENDOR retain online audit records for at least 90 days to provide support for after-the-fact investigations of security incidents and offline for at least one year to meet regulatory and organizational information retention requirements? [AU-11]	X		Please refer to item #5.

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
9	Does the VENDOR have the capability to notify customers and regulators of confirmed incidents in a timeframe consistent with all legal, regulatory, or contractual obligations? The State of NC's requirement for security breach reporting is 24 hrs. of incident confirmation. [IR-6]	X		<p>Please refer to the section "CUSTOMER DATA INCIDENT MANAGEMENT AND NOTIFICATION" in the Data Processing Addendum (DPA) which is part of the Main Services Agreement between both parties. The current standard DPA is available online:</p> <p>https://www.salesforce.com/content/dam/web/en_us/www/documents/legal/Agreements/data-processing-addendum.pdf</p> <p>Salesforce will promptly notify the customer in the event of any security breach of the Service resulting in an actual or reasonably suspected unauthorized disclosure of Customer Data. Different jurisdictions have different requirements, but the notification would likely be faster than any requirement. Notification may include phone contact by Salesforce support, email to customer's administrator and Security Contact (if submitted by customer), and public posting on trust.salesforce.com.</p>
10	If the VENDOR's solution provides email "send as" capabilities, does it support DMARC and DKIM for email protection?			Not Applicable.

3.2.5. Contingency Planning and Disaster Recovery

Only answer "yes" if the answer is consistently "yes." For partially implemented areas, answer "no" and describe what is missing to achieve a "yes" answer. If inherited, please indicate partial or full inheritance in the "Describe Capability" column. Any non-inherited capabilities must be described.

Table 3-6. Contingency Planning and Disaster Recovery

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
1	Does the VENDOR have the capability to recover the system to a known and functional state following an outage, breach, DoS attack, or disaster? [CP-2, CP-9, CP-10]	X		Salesforce has documented Disaster Recovery and Business Continuity plans for critical business functions. The Disaster Recovery and Business Continuity plans are tested at least annually. A postmortem documenting the results of the disaster recovery tests can be provided to customers with a signed NDA in place. The DR/BCP Plan Summary and recent DR postmortem can be requested as a separate request.
2	Does the VENDOR have a Contingency Plan and a fully developed Contingency Plan test plan in accordance with Statewide Information Security Manual? [CP-2, CP-4]	X		Please refer to item #1.
3	Does the system have alternate storage and processing facilities? [CP-6, CP-7]	X		The Disaster Recovery plan is constantly measured against strict regulatory and governance requirements and is a crucial part of the acceptance plan when making changes or additions to the production environment. A key element of the Disaster Recovery plan is Site Switching, which enables the seamless redirection of customer requests from an instance in the primary data center to a replicated instance at a secondary data center. Each instance (for example, NA107 or CS132) contains many servers and other elements to make it run, which is exactly duplicated at the secondary data center. Site Switching minimizes service disruptions when a disaster occurs; it is also useful for minimizing downtime during planned maintenance. The Site Reliability (SR) team plans and conducts regular Site Switching exercises.

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
4	Does the system have or use alternate telecommunications providers? [CP-8]	X		Salesforce is not tied to a single network provider; we can select carriers who deliver the best performance, reliability, and capacity. This design ensures that our customers will experience the shortest access and download times. There is no single point of failure.
5	Does the system have backup power generation or other redundancy? [PE-11]	X		Please refer to item #3.
6	Does the VENDOR have service level agreements (SLAs) in place with all telecommunications providers? [CP-8]	X		Please refer to item #4

3.2.6. Configuration and Risk Management

Only answer "yes" if the answer is consistently "yes." For partially implemented areas, answer "no" and describe what is missing to achieve a "yes" answer. If inherited, please indicate partial or full inheritance in the "Describe Capability" column. Any non-inherited capabilities must be described.

Table 3-7. Configuration and Risk Management

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
1	Does the VENDOR maintain a current, complete, and accurate baseline configuration of the information system? [CM-2]	X		Salesforce has a formal process for placing a system into production (including the hardware, software, and appropriate configuration). This procedure includes a build checklist, server hardening checklist and pre-production testing. Baseline configurations for servers, network devices, and databases are consistent with industry-accepted CIS (Center for Internet Security) system hardening guidelines that address known security vulnerabilities. Prior to go-live with new infrastructure, management approval is required, and the decision is based upon the results of the pre-production testing.
2	Does the VENDOR maintain a current, complete, and accurate inventory of the information system software, hardware, and network components? [CM-8]	X		Salesforce is ISO 27001 certified and asset management is defined through the company's Information Systems Asset Management Policy. This covers items such as acquisition, tracking, ownership, responsibilities, and disposal.
3	Does the VENDOR have a Configuration Management Plan? [CM-9]	X		Please refer to item #1.

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
4	Does the VENDOR follow a formal change control process that includes a security impact assessment? [CM-3, CM-4, CM-4 (2)]	X		Salesforce implements a multipronged approach to ensure the software we release is secure. From initial ideas to release, we deploy several tools and processes in this regard. Specifically, we perform the following tasks to assure security in the development lifecycle.
5	Does the VENDOR employ automated mechanisms to detect inventory and configuration changes? [CM-2, CM-2 (2), CM-6, CM-8]	X		Please refer to item #1.
6	Does the VENDOR prevent unauthorized changes to the system? [CM-5]	X		The limited number of Salesforce employees with administrative access to production systems to manage the infrastructure, are required to authenticate to a secure server using 2 layers of RSA two factor authentication. In the event an administrator enters the wrong PIN/passcode, the system will require the next passcode generated as well, to confirm authentication. The user account will be locked after 10 or more failed login attempts. The account remains locked until it is manually unlocked by another administrator.
7	Does the VENDOR establish configuration settings for products employed that reflect the most restrictive mode consistent with operational requirements? [CM-6, CM-7]	X		Please refer to item #1.
8	Does the VENDOR ensure that checklists for configuration settings are Security Content Automation Protocol (SCAP)-validated or SCAP-compatible (if validated checklists are not available)? [CM-6]	X		

For the following questions, Vendors may use Table 3-18 "Continuous Monitoring Capabilities – Additional Details" to enter the capability descriptions, supporting evidence, and missing elements.

9	Does the VENDOR perform authenticated operating system/ infrastructure, web, and database vulnerability scans at least monthly, as applicable? [RA-5, RA-5 (5)]	X		Salesforce regularly performs self-vulnerability assessments using various tools and techniques, including tools such as Qualys. In addition, Salesforce uses external service providers to perform an application vulnerability assessment after each major release (three times annually) and network vulnerability assessments quarterly. Executive summary reports can be shared upon request and under NDA. Scans are done against applications as well as network type vulnerabilities, such as discovering browser exploits or similar application issues.
10	Does the VENDOR demonstrate the capability to remediate High risk vulnerabilities within 30 days and Moderate risk vulnerabilities within 60 days? [RA-5, SI-2]	X		Salesforce technical operations and security personnel monitor vulnerability alerts and patch release notifications from our vendors and other sources. When a patch is released, it is evaluated by the senior technical and management personnel. The evaluation examines the risk, severity, and mitigation efforts associated with the vulnerability and its associated patch, from which a course of action is prescribed. After initial evaluation, patching follows our Change Management Policy and Procedure, to track, test, and install the update, then notify appropriate internal parties. Depending on the severity and the risk to the Salesforce systems, security patches can be scheduled for immediate deployment or deferred to an appropriate planned maintenance interval. All approved patches are also added to system build images. Additionally, please note that not all patches available for a given application or operating system are necessarily applicable to a particular environment, including Salesforce. This means that patches must be evaluated before installation, not simply loaded at the first possible opportunity.

11	When a High risk vulnerability is identified as part of continuous monitoring activities, does the VENDOR consistently check audit logs for evidence of exploitation? [RA-5]	X		Please refer to item #9.
12	Does the VENDOR have a Supply Chain Risk Management (SCRM) plan and processes to identify and address weaknesses or deficiencies in the supply chain elements and processes of information systems?	X		Agreements with vendors and suppliers contain applicable security requirements which includes requirements for risk assessment within the supply chain.

3.2.7. Data Center Security

Only answer “yes” if the answer is consistently “yes.” For partially implemented areas, answer “no” and describe what is missing to achieve a “yes” answer. If inherited, please indicate partial or full inheritance in the “Describe Capability” column. Any non-inherited capabilities must be described.

Table 3-8. Data Center Security

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
1	Does the VENDOR restrict physical system access to only authorized personnel? [PE-2 through PE-6, PE-8]	X		All access attempts to secured computer rooms are monitored and logged. - Salesforce's Technical Operations data center engineers only have physical access to the servers. Technical Operations management approves physical access to servers and other infrastructure equipment via an internal case. The access list is reviewed on a periodic basis.
2	Does the VENDOR monitor and log physical access to the information system, and maintain access records? [PE-6, PE-8]	X		Please refer to item #1.

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
3	Does the VENDOR monitor and respond to physical intrusion alarms and surveillance equipment? [PE-6, PE-6 (1)]	X		Data centers are monitored using AWS global Security Operations Centers, which are responsible for monitoring, triaging, and executing security programs. They provide 24/7 global support by managing and monitoring data center access activities, equipping local teams and other support teams to respond to security incidents by triaging, consulting, analyzing, and dispatching responses. Physical access points to server rooms are recorded by Closed Circuit Television Camera (CCTV). Images are retained according to legal and compliance requirements. Physical access is controlled at building ingress points by professional security staff utilizing surveillance, detection systems, and other electronic means. Authorized staff utilize multi-factor authentication mechanisms to access data centers. Entrances to server rooms are secured with devices that sound alarms to initiate an incident response if the door is forced or held open.

3.2.8. Policies, Procedures, and Training

The Vendor must indicate the status of policy and procedure coverage for the NIST 800-53 Rev 5 families listed in Table 3-9 below.

To answer “yes” to a policy, it must be fully developed, documented, and disseminated; and it must address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. A single policy document may address more than one family provided the NIST requirements of each “-1” are fully addressed.

To answer “yes” to a procedure, it must be fully developed and consistently followed by the appropriate staff. List all applicable procedure documents for each family.

VENDORS must establish their own set of Policies and Procedures (P&Ps). They cannot be inherited from a leveraged system, nor can they be provided by the customer. Any exceptions and/or missing policy and procedure elements must be explained in Table 3-10 below.

Table 3-9. Policies and Procedures

#	Family	Policy		Procedure		Title Version and Date
		Yes	No	Yes	No	
1	Access Control [AC-1]	X		X		Policy: <ul style="list-style-type: none"> Information Security Policy Procedure(s): <ul style="list-style-type: none"> Blacktab Approval Process Solution IAM Term Process Review Manual Org Deactivations Process Compliance Wireless Scan Review Procedure Termination Process User Guide Production Access Matrix Government Cloud Account Provisioning Process Network Security Account Management Procedure Prolexic Access Management Procedure EMC Access Management Procedure Sourcefire Account Management Procedure Blacktab Access Management Procedure Database Access Management Procedure Security Account Management Procedures SFSS-103 Salesforce – GIA Access Standard
2	Awareness & Training [AT-1]	X		X		Policy: <ul style="list-style-type: none"> Information security Policy Procedure(s): <ul style="list-style-type: none"> Awareness Training Development

#	Family	Policy		Procedure		Title Version and Date
		Yes	No	Yes	No	
3	Audit & Accountability [AU-1]	X		X		Policy: <ul style="list-style-type: none"> Information Security Policy Procedure(s): <ul style="list-style-type: none"> Logging and Auditing Requirements Production Logging Standard CSIRT Monitoring, Auditing and Logging Procedure SR Logging and Monitoring Procedure Network Device Logging Procedure Kerberos Logging Procedure Server Logging Procedure Storage Engineering Team FedRAMP Procedures Database Auditing Procedure Gigamon Logging Procedure
4	Security Assessment & Authorization [CA-1]	X		X		Policy: <ul style="list-style-type: none"> NIST SP 800-37 Procedure(s): <ul style="list-style-type: none"> Continuous Monitoring Plan Assessment and Authorization Process
5	Configuration Management [CM-1]	X		X		Policy: <ul style="list-style-type: none"> Information Security Policy Procedure(s): <ul style="list-style-type: none"> Government Cloud Configuration Guide SFSS-010 Cloud Security Standard Global Service Management – Change Management Policy Production Network Security Standard Infrastructure Hardening Guidelines CIS Hardening Guides – Servers CIS Hardening Guides – Network Devices Salesforce Oracle Hardening Guide Compliance Procedure for AIDE Access Restrictions for Change Compliance Procedure Network Security Account Management Procedure Security Account Management Procedures

#	Family	Policy		Procedure		Title Version and Date
		Yes	No	Yes	No	
6	Contingency Planning [CP-1]	X		X		Policy: <ul style="list-style-type: none"> Information Security Policy Procedure(s): <ul style="list-style-type: none"> Technology Operations Disaster Recovery (DR) Plan Production Disaster Recovery Runbooks
7	Identification & Authentication [IA-1]	X		X		Policy: <ul style="list-style-type: none"> Information Security Policy Procedure(s): <ul style="list-style-type: none"> Infrastructure Authentication Path Diagram Changing Kerberos Passwords from SGD Network Security Account Management Procedure Security Account Management Procedures
8	Incident Response [IR-1]	X		X		Policy: <ul style="list-style-type: none"> Information Security Policy Procedure(s): <ul style="list-style-type: none"> SFSS-010 Incident Response Standard Security Incident Response Plan
9	Maintenance [MA-1]	X		X		Policy: <ul style="list-style-type: none"> Information Security Policy Procedure(s): <ul style="list-style-type: none"> Global Service Management - Change Management Policy Remote maintenance Procedure
10	Media Protection [MP-1]	X		X		Policy: <ul style="list-style-type: none"> Information Security Policy Third-Party Data Handling Standard Procedure(s): <ul style="list-style-type: none"> Media Handling Process

#	Family	Policy		Procedure		Title Version and Date
		Yes	No	Yes	No	
11	Physical & Environmental Protection [PE-1]					
12	Personnel Security [PS-1]					<ul style="list-style-type: none">Information Security PolicyPersonnel Security for ContractorsPersonnel Security for Employees
13	Risk Assessment [RA-1]	X		X		Policy: <ul style="list-style-type: none">NIST 800-30 Procedure(s): <ul style="list-style-type: none">SFSS-090 Vulnerability RankingVulnerability Identification ProcessApplication Security Assessment Procedures
14	System & Services Acquisition [SA-1]	X		X		Policy: <ul style="list-style-type: none">Information Security Policy Procedure(s): <ul style="list-style-type: none">Product Security Feature LifecycleGlobal Service Management - Change management PolicyVendor Assessments
15	System & Communications Protection [SC-1]	X		X		Policy: <ul style="list-style-type: none">Information Security Policy Procedure(s): <ul style="list-style-type: none">Information Security Technical StandardsNetwork Layer Tour GuideCompliance Procedure for AIDESecurity Incident Response PlanEncryption and Key Management Policy

#	Family	Policy		Procedure		Title Version and Date
		Yes	No	Yes	No	
16	System & Information Integrity [SI-1]	X		X		Policy: <ul style="list-style-type: none"> Information Security Policy Procedure(s): <ul style="list-style-type: none"> Security Incident Response Plan Compliance Procedure for AIDE SFDC Vulnerability Severity Ranking DISMA POA&M Security Directives Production Anti-Virus Procedure Production File Integrity Monitoring Procedure CSIRT Monitoring, Auditing, and Logging Security Patch Management SFSS-027 Patch Management
17	Planning [PL-1]	X		X		Policy: <ul style="list-style-type: none"> NIST 800-18
18	Supply Chain Risk Management [SR-1]	X		X		Policy: <ul style="list-style-type: none"> Document TBD as this SR-1 is a NIST SP 800-53 Rev. 5 control. This document is still in progress. Procedure(s): <ul style="list-style-type: none"> Salesforce Security Plan (SA-12)

For any family with a policy or procedure gap, please describe the gap below.

Table 3-10. Missing Policy and Procedure Elements

Missing Policy and Procedure Elements
•

The Vendor must answer the questions below.

Table 3-11. Security Awareness Training

Question	Yes	No	Describe capability, supporting evidence, and any missing elements
Does the VENDOR train personnel on security awareness and role-based security responsibilities? [AT-2]	X		<p>Information security policies are published on Salesforce's internal portal available to all employees and contractors and communicated to personnel through internal training and awareness campaigns. Policy training is conducted upon hire and annually thereafter.</p> <p>All employees undergo a Security Awareness training session in a classroom setting as part of our New Employee Orientation. This class includes an introduction to security topics, Salesforce policies, employee procedures, and includes a sign off on understanding.</p>

		<p>All employees participate in an annual training and re-certification security awareness program which is conducted by way of an online computer based training and learning management system. These courses include testing and sign-off/attestation of understanding and agreement. Training history is captured in our learning management system upon completion.</p> <p>Additional supplemental Security Awareness material is provided via email bulletins/updates and/or newsletters to employees.</p> <p>Secure coding training (e.g., OWASP, CERT) for all developers is in place and applied as part of the systems development life cycle process SSDL training in place.</p>
--	--	---

3.3. Additional Capability Information

State will evaluate the responses in this section on a case-by-case basis relative to a State-Ready designation decision.

3.3.1. Staffing Levels

*In the table below, the Vendor must describe the VENDOR’s organizational structure, staffing levels currently dedicated to the security of the system, as well as any planned changes to these staffing levels. This description must clearly indicate role and number of individuals as well as identify which staff is full-time dedicated, and which are performing their role as a collateral duty. **Note:** It is not necessary to include specific names of individuals, but rather their roles/titles.*

Table 3-12. Staffing Levels

Staffing Levels
Salesforce does not publish details on the number of employees operating within different departments. A general description on the structure of the company is included in our annual report (10K), which is found on our investor relations website: http://investor.salesforce.com/about-us/investor/financials/default.aspx
Please refer to https://investor.salesforce.com/corporate-governance/default.aspx

3.3.2. Change Management Maturity

While the following change management capabilities are not required, they indicate a more mature change management capability and may influence a State Readiness decision, especially for larger systems.

The Vendor must answer the questions below.

Table 3-13. Change Management

#	Question	Yes	No	If "no", please describe how this is accomplished.
1	Does the VENDOR's change management capability include a fully functioning Change Control Board (CCB)?	X		Network and infrastructure change control procedures are required by the company's Change Management Policy and include steps for testing, review, authorization, communication, verification, and backout procedures. All changes to the infrastructure components are tested in a dedicated environment using production class equipment before being deployed into production. An Emergency change process is also in place. Changes are reviewed and approved by Technical Operations management prior to deployment to production. System changes and maintenance are managed using an internal case tracking system. Vendor-supplied OS, application, and networking patches are evaluated by systems administrators, tested on internal systems, and are deployed by Technical Operations during announced maintenance periods.

#	Question	Yes	No	If "no", please describe how this is accomplished.
2	Does the VENDOR have and use development and/or test environments to verify changes before implementing them in the production environment?	X		<p>Once the code is checked in, the bug is transferred from the developer to a QA Engineer, who is responsible for unit testing again, as well as integration testing the change. Concurrently, nightly builds are performed, and full regression tests run using the appropriate automated test. Once code is frozen prior to a major release, there are "bug blitzes" in which all members of QA, Development, and Product Management participate. During these blitzes, every person is assigned a list of features to test, as well as a test plan for each.</p> <p>Automated Testing Salesforce uses automated testing to cover a broad range of code checks. Automated testing allows for quick sanity checking and near real-time notification of regressions within our system. Testing tools include: - Unit testing - Code coverage - User Interface functional testing - Web application security Internal User Testing We also are committed to user testing, which includes corner cases with particular data settings mimicked from the production environment.</p>

3.3.3. Vendor Dependencies and Agreements

The Vendor must answer the questions below.

Table 3-14. Vendor Dependencies and Agreements

#	Question	Yes	No	Instructions
1	Does the system have any dependencies on other vendors such as a leveraged service offering, hypervisor and operating system patches, physical security and/or software and hardware support?	X		If "yes," please complete Table 3-15. Vendor Dependencies below.
2	Within the system, are all products still actively supported by their respective vendors?	X		If any are not supported, answer, "No."
3	Does the VENDOR have a formal agreement with a vendor, such as for maintenance of a leveraged service offering?	X		If "yes," please complete Table 3-16. Formal Agreements Details below.

If there are vendor dependencies, please list each in the table below, using one row per dependency. For example, if using another vendor's operating system, list the operating system, version, and vendor name in the first column, briefly indicate the VENDOR's reliance on that vendor for patches, and indicate whether the vendor still develops and issues patches for that product. If there are no vendor dependencies, please type "None" in the first row.

3.3.4. Continuous Monitoring Capabilities

In the tables below, please describe the current state of the VENDOR's Continuous Monitoring capabilities, as well as the length of time the VENDOR has been performing Continuous Monitoring for this system.

Table 3-17. Continuous Monitoring Capabilities

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
1	Does the VENDOR have a lifecycle management plan that ensures products are updated before they reach the end of their vendor support period?	X		Security is and always will be the top priority of the company. To help meet the expectations our customers have in Salesforce to be the trusted provider of enterprise

			<p>business services, we have built security into our development processes at all stages. From initial architecture considerations to post release, all aspects of these practices have built-in security. Later in this section, you'll find some of the standard practices employed at Salesforce, which have made Salesforce the trust provider it is today.</p> <p>Secure Design</p> <ul style="list-style-type: none">● Salesforce has built its security program around ten guiding security principles, adapted from the OWASP Secure Coding Principles. These principles lead out technologists to make the best security decisions possible for our customer base to ensure customer trust.● All Salesforce developer and QA staff are trained on security best practices. New hires are required to be trained within their first month of employment. The training covers the basics of application security - such as the OWASP Top 10. Additionally, in depth training and labs are available to employees.● Threat assessments are performed on all high-risk features during the design. These assessments help identify potential security issues early on in the development process and also help the QA team perform focused security testing during the release. <p>Secure Coding</p> <ul style="list-style-type: none">● During development of
--	--	--	--

			<p>features, developers utilize the valuable techniques identified during training to build security into their features. Secure coding patterns and anti-patterns exist that cover standard vulnerability types such as the OWASP Top 10 and CWE 25 have been written and are updated frequently to cover standard and sometimes obscure vulnerabilities types.</p> <ul style="list-style-type: none"> • Several static code analysis tools are run through the release process. HP Fortify, Checkmarx, FindBugs and several proprietary code analysis tools are used to identify security flaws as early on in the development process as possible. <p>Certain potentially dangerous function calls within Salesforce are not approved for use. Specifically, those that pull user input from query strings, forms, or other areas must use Salesforce's approves method for doing so which requires the developer to use an approved validation pattern to assure the data is of the correct type, length, and format. The tools previously mentioned are used to catch cases where this is not done correctly.</p>
2	Does the VENDOR have the ability to scan all hosts in the inventory?	X	<p>Internal Vulnerability Assessment</p> <p>Salesforce regularly performs self-vulnerability assessments using various tools and techniques, including tools such as Qualys.</p> <p>Third-party Vulnerability Assessments</p> <p>Salesforce uses external service providers to perform</p>

			<p>an application vulnerability assessment after each major release (three times annually) and network vulnerability assessments quarterly. Executive reports for these assessments are available for customers (under NDA) upon request.</p> <p>Applications Assessments</p> <p>Applications tests probe possible vulnerabilities in the program components and technologies served by Salesforce:</p> <ul style="list-style-type: none">- Analysis of Authentication Mechanism- Observes the handling of usernames and passwords. Tests account password strength and lockout settings. Ensures that usernames cannot be revealed passed on failed login attempts. Ensures that the site supports options for strong password handling and change.- Observed Use of Encryption- Ensures that all transmissions of sensitive data are encrypted. Verifies that weak key exchange protocols are not supported on the server.- SQL Injection- Attempts to inject SQL commands into the back-end database. A successful attack may lead to unauthorized access to the system.- HTML Source Analysis- Parses the HTML code for exploitable tags. For example, hidden form fields can be used to obtain access to data without authorization.- Cross-Site Scripting- Identifies the ability to inject client-side scripts into a
--	--	--	---

			<p>publicly viewable area of the site. Other users may then execute the code, revealing cookies and other information. This also includes the ability for an attacker to forward the user to another site containing a cross-site scripting attack (URL redirection).</p> <ul style="list-style-type: none">- Frame Manipulation- Ensures that the site cannot be encapsulated as a frame in another site.- Buffer Overflows- Verifies that attempts to send excess data to a field of limited size don't compromise the system or reveal sensitive data.- Cookie Analysis- Ensures that no critical information can be manipulated in the cookie and that the cookie has the secure flag set to protect sensitive data stored within.- Session Handling- Verifies that the site has appropriate settings for session handling and inactivity timeout.- Privilege Enforcement- Verifies that users may not escalate their privilege level or read/write data belonging to another user.- File Upload/Download- Ensures that data transfers such as file uploading and downloading may not be manipulated to gain access to additional data or be used to upload malicious content.- Email Functions- Ensures that all email contact functions may not be manipulated to facilitate an email spoofing attack.- Common Web Server Vulnerabilities- Verifies that
--	--	--	---

			<p>commonly known web server vulnerabilities are not present (such as those listed in the CVE database).</p> <p>Network Vulnerability Assessments</p> <p>Environment tests use automated tools to scan and identify vulnerabilities in the target environment, then include a manual follow-up to provide thorough coverage:</p> <ul style="list-style-type: none">- Live Host Identification- TCP and ICMP "ping sweeps" identify the live hosts (and their IP addresses) on each subnet.- Host and Service Identification - Identify specific system and application information on the networks, including open ports, operating system types and versions, available services, and the applications providing those services. This information is correlated with known or emerging vulnerabilities to establish the basis for further testing.- Manual Verification- Examine results from the automated tools to identify any false positives and some complex, emerging, or obscure vulnerabilities that may provide an entry point for penetrating the network. <p>Bug Bounty</p> <p>Salesforce operates a private 'Bug Bounty' program. Security researchers are invited to identify and responsibly disclose potential security vulnerabilities to Salesforce.</p> <p>Vulnerability Remediation</p> <p>All bugs discovered during</p>
--	--	--	--

			<p>third-party assessments are documented and tracked using Salesforce's standard bug tracking system. Remediation of the flaws is dependent on the severity and cost of the fix. While most issues are addressed very quickly, the lower severity issues are reviewed every release and re-prioritized as necessary. Salesforce does manual testing on the fix and if possible, writes an automation script that assures the issue is tested for in the future.</p> <p>External independent scans can also be coordinated with the Salesforce team as needed.</p>
--	--	--	--

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
3	Does the VENDOR have the ability to provide scan files in a structure data format, such as CSV, XML files?	X		Executive summary reports can be shared upon request and under NDA.
4	Is the VENDOR properly maintaining their Plan of Actions and Milestones (POA&M), including timely, accurate, and complete information entries for new scan findings, vendor check-ins, and closure of POA&M items?	X		Salesforce's complete FedRAMP Authority to Operate (ATO) package for the Salesforce Government Cloud contains the following weakness remediation documentation: - Salesforce Government Cloud Plan of Action and Milestones (POA&M)

In the table below, provide any additional details the Vendor believes to be relevant to State's understanding of the VENDOR's Continuous Monitoring Capabilities. If the Vendor has no additional details, please state, "None."

Table 3-18. Continuous Monitoring Capabilities – Additional Details

Continuous Monitoring Capabilities – Additional Details
Can the vendor provide a current 3rd party attestation certification <u>annually</u> when required? Note: SaaS vendors cannot use IaaS/PaaS certification unless the application is explicitly covered as part of the IaaS/PaaS assessments. [CA-7, RA-3, SA-9]
Yes. Salesforce has comprehensive privacy and security assessments and certifications performed by multiple third parties. The following audits and their frequencies are performed: - ISO 27001 - Annually (with 3-year certification) - ISO 27018 - Annually - PCI-DSS - Annually - FedRAMP - Annually - SOC 1 (SSAE16 /ISAE 3402, previously SAS 70) - Twice a year - SOC 2 & SOC 3 - Twice a year

3.3.5. Status of System Security Plan (SSP)

In the table below, explicitly state whether the SSP is fully developed, partially developed, or non-existent. Identify any sections that the VENDOR has not yet developed.

Table 3-19. Maturity of the System Security Plan

Maturity of the System Security Plan
Fully developed.

In the table below, state the number of controls identified as "Not applicable" in the SSP. List the Control Identifier for each, and indicate whether a justification for each has been provided in the SSP control statement.

Table 3-20. Controls Designated "Not Applicable"

<x> Controls are Designated "Not Applicable"

In the table below, state the number of controls with an alternative implementation. List the Control

Identifier for each.


Table 3-21. Controls with an Alternative Implementation

<x> Controls have an Alternative Implementation

Salesforce is an innovative cloud services provider with evolving technology. Salesforce has made a good faith effort to provide you with responses to your request that are accurate as of the date of the response and within our knowledge. Because Salesforce procedures and policies change from time to time, and Salesforce continues to innovate by providing each customer multiple major release upgrades each year, we cannot guarantee that the answers to your request will remain the same over time. The rights and responsibilities of the parties with regard to your purchase and/or use of Salesforce's online software services and/or Salesforce's performance of professional services shall be set forth solely in the applicable agreement(s) executed by Salesforce, including its provision that any purchases thereunder are not contingent on the delivery of any future functionality or features, or dependent on any oral or written public comments made by Salesforce regarding future functionality or features. The responses herein shall not be part of a final contract. All information provided herein is deemed Salesforce Confidential Information and subject to the confidentiality terms contained in the agreements between you and Salesforce, and/or its authorized Salesforce reseller, and shall be exempt from disclosure to the maximum extent permitted by applicable law.

Organization's Security Representative or designee

Print Name Evan Danner

DocuSigned by:

753C910EDD1D484...
SIGNATURE

Date July 11, 2023



Section f)

Architecture Diagrams

f) Architecture Diagrams

3.3.2 ARCHITECTURE DIAGRAMS DEFINED

The State utilizes architectural diagrams to better understand the design and technologies of a proposed solution. These diagrams (i.e., Network Diagram and Technology Stack Diagram), required at offer submission, can be found at the following link: <https://it.nc.gov/architectural-artifacts>.) There may be additional architectural diagrams requested of the vendor after contract award. This will be communicated to the vendor by the agency as needed during the project.

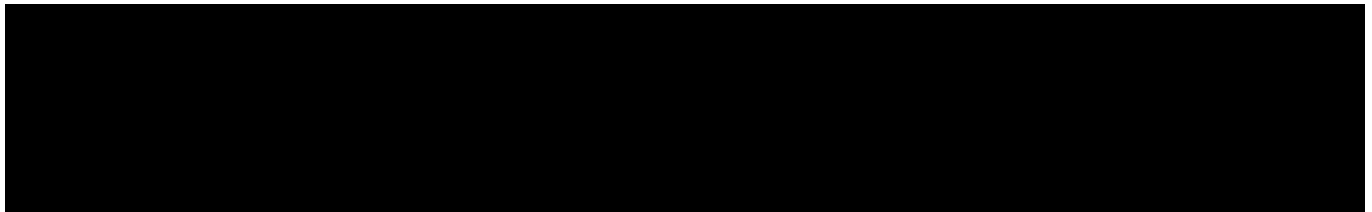
Network Architecture Diagram

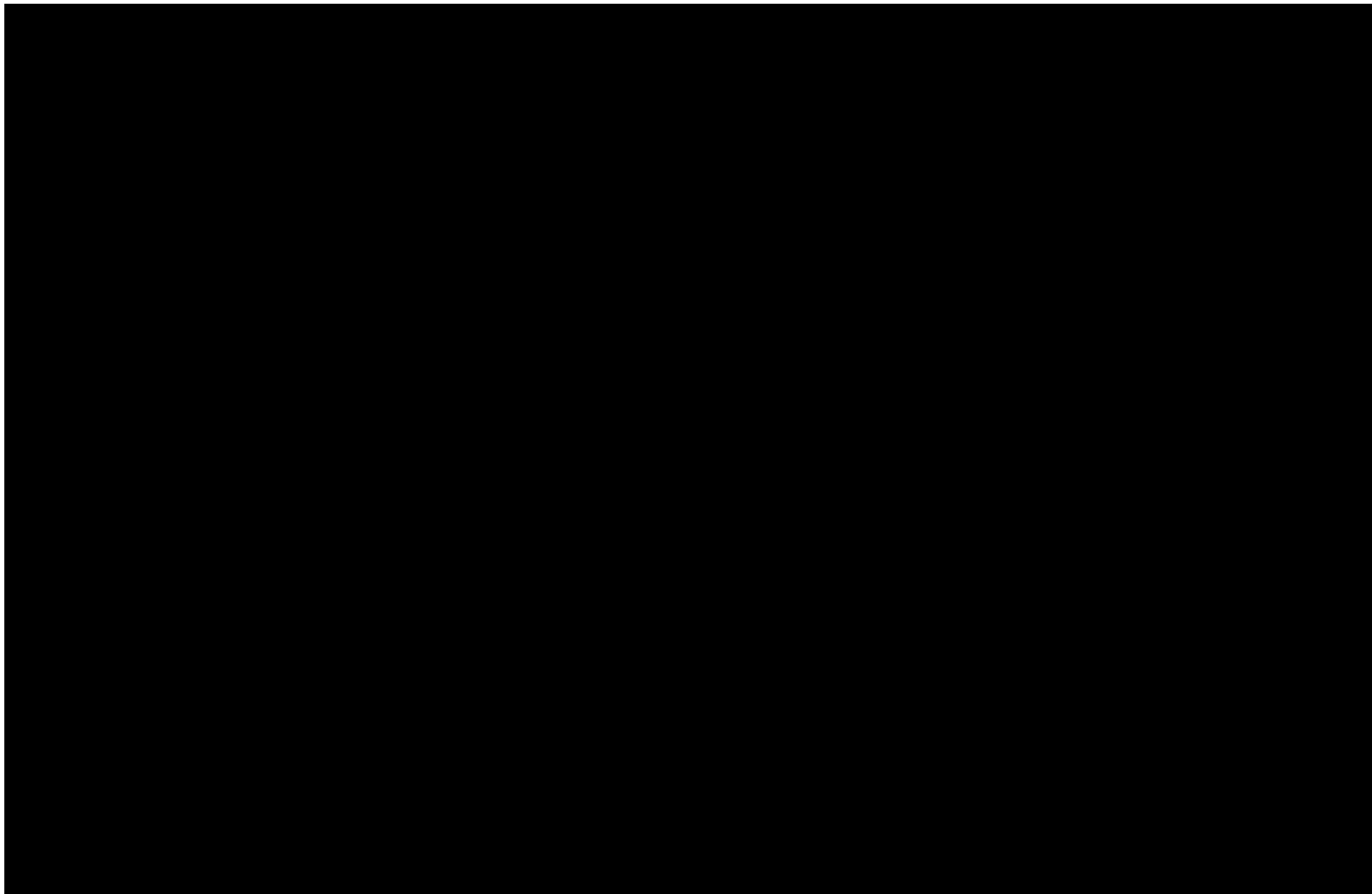
This diagram describes the means of communication, the method of sending and receiving information, between the assets in the Technology Architecture. The diagram will take logical connections between client and server components and identify network boundaries and network infrastructure required to physically implement those connections. It does not describe the information format or content but will address protocol and capacity issues.

The network architecture will be finalized during the project's Discovery phase. Accenture proposes using Salesforce, a cloud-based SaaS platform, integrated with the depicted technology stack.

Technology Stack Diagram

Technology stack, also called a solution stack, is a set of software components that compose a logically complete platform for running a service or supporting an application. It is the set of software that provides the infrastructure for a solution. The stacks differ based on the deployment location (e.g., client, server, mainframe). The technology stack diagram depicts the relationships and critical communication paths between the solution's software components.







Section g)

Cost Form for Vendor's Offer (Attachment E)

g) Cost Form for Vendor's Offer (Attachment E)

4.1 Offer Costs

The Vendor must list, itemize, and describe any applicable offer costs which may include the following

- a) Software License fees or costs to accommodate user base identified.
- b) Additional modules required or proposed addressing specifications, if any.
- c) Third-party software, if any, required for the operation of the Solution.
- d) Installation/configuration/integration/transition costs.
- e) Customization required or proposed addressing specifications: The costs for customization shall be detailed on an attachment by item and cost for each customization to the Vendor product
- f) Conversion and migration of legacy data.
- g) Deliverables in accordance with Section 3.5.2 Table 1: Project Execution and/or O&M Deliverables and Responsibilities, and Attachment J: Minimum Content for Project and O&M Deliverables, including updates and revisions.
- h) Training and training materials.
- i) Annual maintenance and Vendor hosting costs per contract year, if not included in Software License Costs.
- j) Customer Support to include Help Desk and Technical Support costs per contract year, if not included in annual maintenance costs or Software License Costs.
- k) Escrow costs (If COTS products are included in the Solution).
- l) Cost of Change Hours per year.
- m) Other costs shall be listed separately by type of service/cost as an attachment. List separately any changes associated with State hosting. Travel and lodging expenses, if any, must be thoroughly described, and are limited by the State's Terms and Conditions.
- n) Hourly rate for additional professional services such as consulting and other value-added services provided the Vendor upon request by the Division.

In section g) 'Cost of Vendor's offer', we've detailed the pricing components as specified in the RFP and consistent with our proposal. As requested, we've distinguished between Project Execution costs and O&M phase costs. We've summarized the costs for all 5 contract years requested. The final table presents the hourly rate for vendor's value-added services, available upon the Division's request for each contract year.

Cost Table 1: Project Execution

Cost Table 1 reflects total cost of software and licensing fees and all implementation costs for the entire project execution phase

Item	Cost Category	Per Unit Cost	Extended Cost All Units	Optional Cost	Project Subtotal
1	Software and Licensing Fees for Year 1 *	N/A	N/A	N/A	\$ 518,882
2	Additional Modules required/proposed for Year 1	N/A	N/A	N/A	N/A
3	Third-party Software for Year 1	N/A	N/A	N/A	N/A
4	Installation/configuration/ integration/ transition costs	N/A	N/A	N/A	\$ 5,250,000
5	Customization required or proposed addressing specifications (itemize in an attachment) **	N/A	N/A	N/A	N/A
6	Conversion and migration of Legacy Data	N/A	N/A	N/A	\$ 450,000
7	Project Deliverables (excluding Data Conversion, Training Materials, Training, and Escrow agreement)	N/A	N/A	N/A	\$ 1,200,000
8	Training and Training Materials	N/A	N/A	N/A	\$ 600,000
9	Customer Support to include Help Desk and Technical Support, if not included in Software License	N/A	N/A	N/A	N/A
10	Escrow	N/A	N/A	N/A	N/A
11	Change Hours (400 hours) for Year 1 ***	\$ 185	\$ 74,000	N/A	\$ 74,000
12	Other Costs (itemize in an attachment)	N/A	N/A	N/A	N/A
Project Execution Subtotal		N/A	\$ 74,000	N/A	\$ 8,092,882
13.a	Annual Maintenance and State Hosting Option (Contract Year 1)	N/A	N/A	N/A	N/A
13.b	Annual Maintenance and Vendor Hosting Option if not included in License fees (Contract Year 1)	N/A	N/A	N/A	N/A
Project Execution Total – Vendor Hosting		N/A	\$ 74,000	N/A	\$ 8,092,882
Project Execution Total – State Hosting		N/A	N/A	N/A	N/A

Cost Table 2: Operations and Maintenance

Provide the firm, fixed O&M cost, inclusive of all O&M tasks and the Software License cost for each year during O&M. If a cost category (or column) is not relevant for the proposed Solution, indicate with "N/A" in the appropriate row/column. The cost for partial years of O&M will be prorated.

Item	Cost Category	Year 1	Year 2	Year 3	Year 4	Year 5	O&M Sub-total
1	Software and Licensing Fees *	See Table 1	\$ 853,501	\$ 1,192,797	\$ 1,231,743	\$ 1,272,080	\$ 4,550,121
2	Additional Modules	See Table 1	N/A	N/A	N/A	N/A	N/A
3	Third-party Software	See Table 1	N/A	N/A	N/A	N/A	N/A
4	Installation/ configuration/ integration/ transition costs addressing Priority 2 specifications (itemize in an attachment)	See Table 1	N/A	N/A	N/A	N/A	N/A
5	Customization required or proposed addressing Priority 2 specifications (itemize in an attachment)	See Table 1	N/A	N/A	N/A	N/A	N/A
6	Conversion and migration of Legacy Data	See Table 1	N/A	N/A	N/A	N/A	N/A
7	Project Deliverables (excluding Data Conversion, Training Materials, Training, and Escrow agreement)	See Table 1	N/A	N/A	N/A	N/A	N/A
8	Training and Training Materials	See Table 1	N/A	N/A	N/A	N/A	N/A
9	Customer Support to include Help Desk and Technical Support, if not included in Software License	See Table 1	\$ 2,196,000	\$ 1,782,000	\$ 1,518,000	\$ 1,593,600	\$ 7,089,600
10	Escrow	See Table 1	N/A	N/A	N/A	N/A	N/A
11	Change Hours (200 hours) ***	See Table 1	\$ 37,000	\$ 37,000	\$ 41,000	\$ 41,000	\$ 156,000
12	Other Costs (itemize in an attachment)	See Table 1	N/A	N/A	N/A	N/A	N/A
O&M Subtotal		See Table 1	\$ 3,086,501	\$ 3,011,797	\$ 2,790,743	\$ 2,906,680	\$ 11,795,721
13.a	Annual Maintenance and State Hosting Option		N/A	N/A	N/A	N/A	N/A
13.b	Annual Maintenance and Vendor Hosting Option if not included in License fees		N/A	N/A	N/A	N/A	N/A
Project Execution Total – Vendor Hosting		See Table 1	\$ 3,086,501	\$ 3,011,797	\$ 2,790,743	\$ 2,906,680	\$ 11,795,721
Project Execution Total – State Hosting							

Cost Table 3: Total Cost of Contract

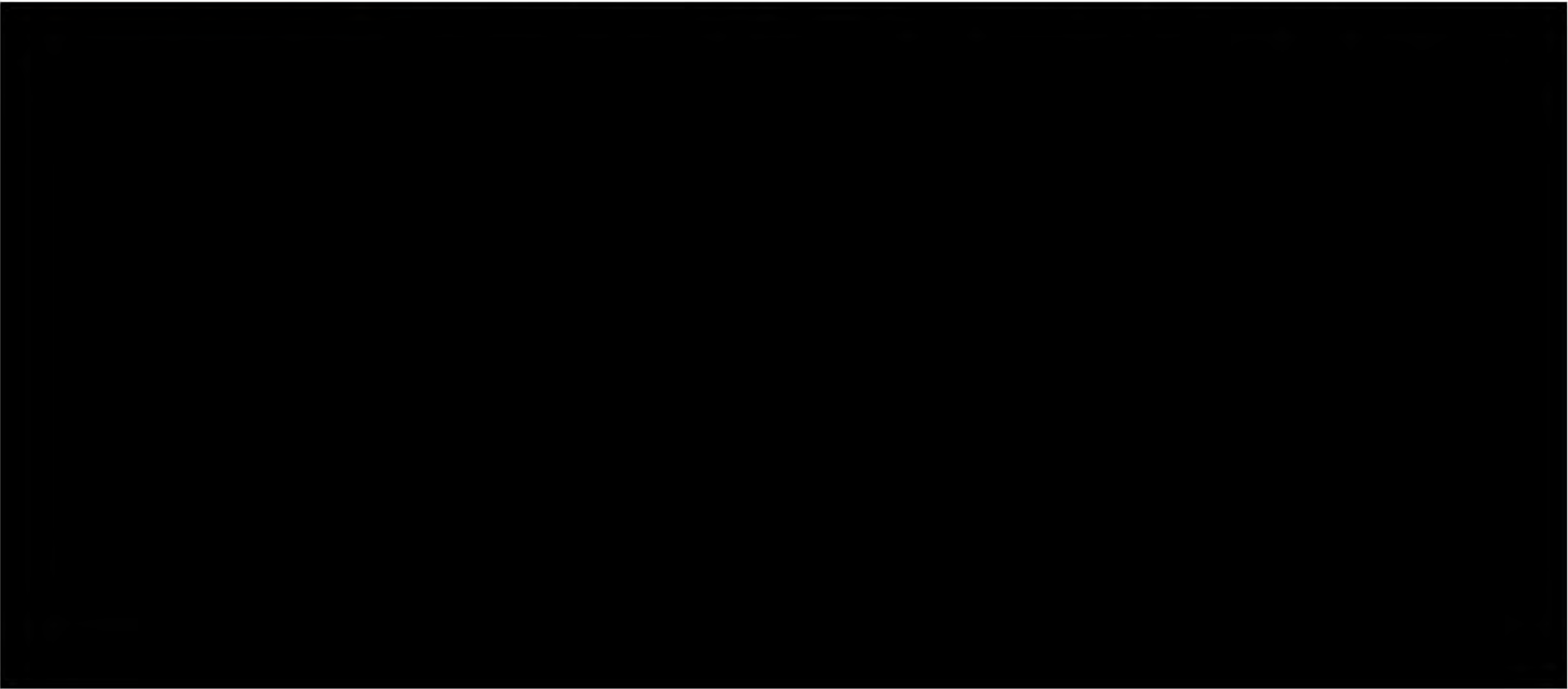
Cost Table 3 provides a summary of the Total Cost of the Contract for five (5) years.

Item	Cost Category	Project Execution Total	O&M Total	Grand Total
1	Software and Licensing Fees	\$ 518,882	\$ 4,550,121	\$ 5,069,003
2	Additional Modules	N/A	N/A	N/A
3	Third-party Software	N/A	N/A	N/A
4	Installation/ configuration/ integration/ transition costs	\$ 5,250,000	\$ -	\$ 5,250,000
5	Customization required or proposed addressing Priority 2 specifications (itemize in an attachment)**	N/A	N/A	N/A
6	Conversion and migration of Legacy Data	\$ 450,000	N/A	\$ 450,000
7	Project Deliverables (excl. Data Conversion, Training Materials, Training, and Escrow agmt)	\$ 1,200,000	N/A	\$ 1,200,000
8	Training and Training Materials	\$ 600,000	N/A	\$ 600,000
9	Customer Support to include Help Desk and Technical Support	N/A	\$ 7,089,600	\$ 7,089,600
10	Escrow	N/A	N/A	N/A
11	Change Hours***	\$ 74,000	\$ 156,000	\$ 230,000
12	Other Costs (itemize in an attachment)	N/A	N/A	N/A
O&M Subtotal		\$ 8,093,306	\$ 11,797,604	\$ 19,890,910
13.a	Annual Maintenance and State Hosting Option	N/A	N/A	N/A
13.b	Annual Maintenance and Vendor Hosting Option if not included in License fees	N/A	N/A	N/A
O&M Total – Vendor Hosting		\$ 8,092,882	\$ 11,795,721	\$ 19,888,603

Cost Table 4: Professional Services Hourly Rate

List the hourly rate for value-added services provided by the Vendor upon request by the Division for each Contract year.

It.	Cost Category	Year 1	Year 2	Year 3	Optional Year 4	Optional Year 5	Total
1	Professional Services Hourly Rate	\$ 177	\$ 185	\$ 192	\$ 201	\$ 209	\$ 964



4.2 Payment Schedule

The Vendor shall propose its itemized payment schedule based on the content of its offer. All payments must be based upon acceptance of one or more Deliverables.

The tables below outline an expected payment plan for the implementation scope outlined. This is a chronological view of the overall cost breakdown in five milestones followed by the Operations and Maintenance monthly fees. As per the RFP required, a 10% retainage is applied to billing associated to deliverables.

Project Execution Phase Payment Schedule

Item #	Project Execution Phase Deliverables	Estimated Invoice Month	Fees	Less 10% Retainage	Payment Amount
1		Month 02	\$ 81,820	\$ -	\$ 81,820
2		Month 02	\$ 275,000	\$ 27,500	\$ 247,500
3		Month 02	\$ 75,000	\$ 7,500	\$ 67,500
4		Month 02	\$ 75,000	\$ 7,500	\$ 67,500
5		Month 02	\$ 75,000	\$ 7,500	\$ 67,500
6		Month 02	\$ 75,000	\$ 7,500	\$ 67,500
7		Month 02	\$ 75,000	\$ 7,500	\$ 67,500
8		Month 02	\$ 65,000	\$ -	\$ 65,000
	Phase				
9		Month 03	\$ 81,818	\$ -	\$ 81,818
10		Month 03	\$ 275,000	\$ 27,500	\$ 247,500
11		Month 03	\$ 75,000	\$ 7,500	\$ 67,500
12		Month 03	\$ 112,500	\$ 11,250	\$ 101,250
13		Month 03	\$ 150,000	\$ 15,000	\$ 135,000
14		Month 04	\$ 81,818	\$ -	\$ 81,818
15		Month 04	\$ 275,000	\$ 27,500	\$ 247,500
16		Month 04	\$ 150,000	\$ 15,000	\$ 135,000
17		Month 04	\$ 150,000	\$ 15,000	\$ 135,000
18		Month 04	\$ 118,750	\$ -	\$ 118,750
	Phase				
19		Month 05	\$ 81,818	\$ -	\$ 81,818
20		Month 05	\$ 275,000	\$ 27,500	\$ 247,500
21		Month 05	\$ 300,000	\$ 30,000	\$ 270,000
22		Month 05	\$ 112,500	\$ 11,250	\$ 101,250
23		Month 05	\$ 150,000	\$ 15,000	\$ 135,000
24		Month 06	\$ 81,818	\$ -	\$ 81,818
25		Month 06	\$ 275,000	\$ 27,500	\$ 247,500

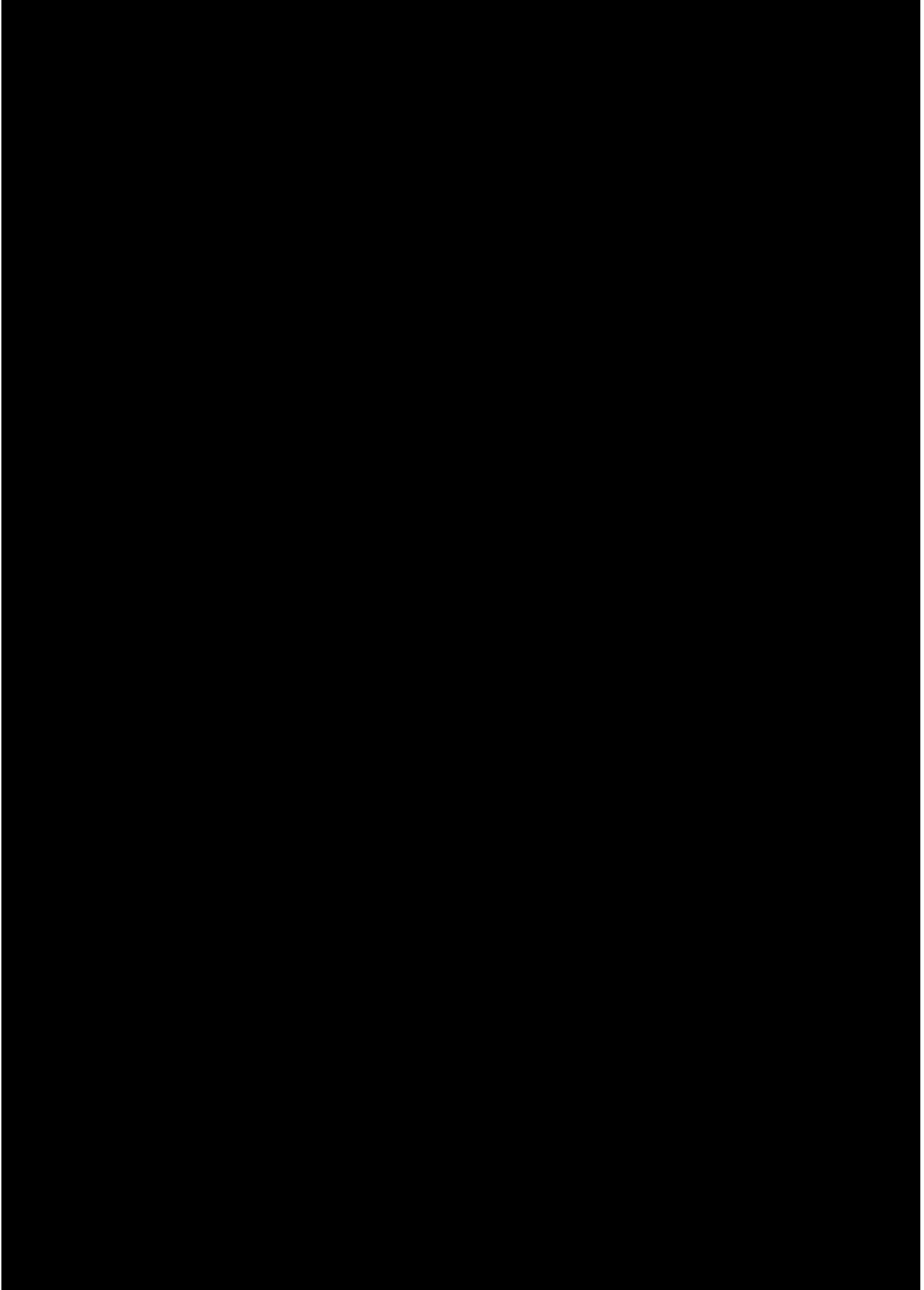
Item #	Project Execution Phase Deliverables	Estimated Invoice Month	Fees	Less 10% Retainage	Payment Amount	
26	Project Execution Phase Deliverables	Month 06	\$ 225,000	\$ 22,500	\$ 202,500	
27		Month 06	\$ 75,000	\$ 7,500	\$ 67,500	
28		Month 06	\$ 225,000	\$ 22,500	\$ 202,500	
29		Month 07	\$ 81,818	\$ -	\$ 81,818	
30		Month 07	\$ 275,000	\$ 27,500	\$ 247,500	
31		Month 07	\$ 225,000	\$ 22,500	\$ 202,500	
32		Month 07	\$ 75,000	\$ 7,500	\$ 67,500	
33		Month 07	\$ 75,000	\$ 7,500	\$ 67,500	
34		Month 08	\$ 81,818	\$ -	\$ 81,818	
35		Month 08	\$ 275,000	\$ 27,500	\$ 247,500	
36		Month 08	\$ 150,000	\$ 15,000	\$ 135,000	
37		Month 08	\$ 225,000	\$ 22,500	\$ 202,500	
38		Month 09	\$ 81,818	\$ -	\$ 81,818	
39		Month 09	\$ 275,000	\$ 27,500	\$ 247,500	
40		Month 09	\$ 112,500	\$ 11,250	\$ 101,250	
41		Month 09	\$ 93,750	\$ 9,375	\$ 84,375	
42		Month 09	\$ 93,750	\$ 9,375	\$ 84,375	
43		Month 10	\$ 81,818	\$ -	\$ 81,818	
44		Month 10	\$ 275,000	\$ 27,500	\$ 247,500	
45		Month 10	\$ 75,000	\$ 7,500	\$ 67,500	
46		Month 10	\$ 93,750	\$ 9,375	\$ 84,375	
47		Month 10	\$ 93,750	\$ 9,375	\$ 84,375	
48		Month 10	\$ 405,000	\$ -	\$ 405,000	
			End of Phase			
49			Month 11	\$ 81,818	\$ -	\$ 81,818
50			Month 11	\$ 75,000	\$ 7,500	\$ 67,500
51			Month 11	\$ 112,500	\$ 11,250	\$ 101,250
52			Month 11	\$ 93,750	\$ 9,375	\$ 84,375
53			Month 11	\$ 93,750	\$ 9,375	\$ 84,375
54			Month 12	\$ 81,818	\$ -	\$ 81,818
55		Month 12	\$ 75,000	\$ 7,500	\$ 67,500	
56		Month 12	\$ 93,750	\$ 9,375	\$ 84,375	
57		Month 12	\$ 93,750	\$ 9,375	\$ 84,375	
58		Month 12	\$ 75,000	\$ 7,500	\$ 67,500	
59		Month 12	\$ 71,250	\$ -	\$ 71,250	
		\$7,500,000				

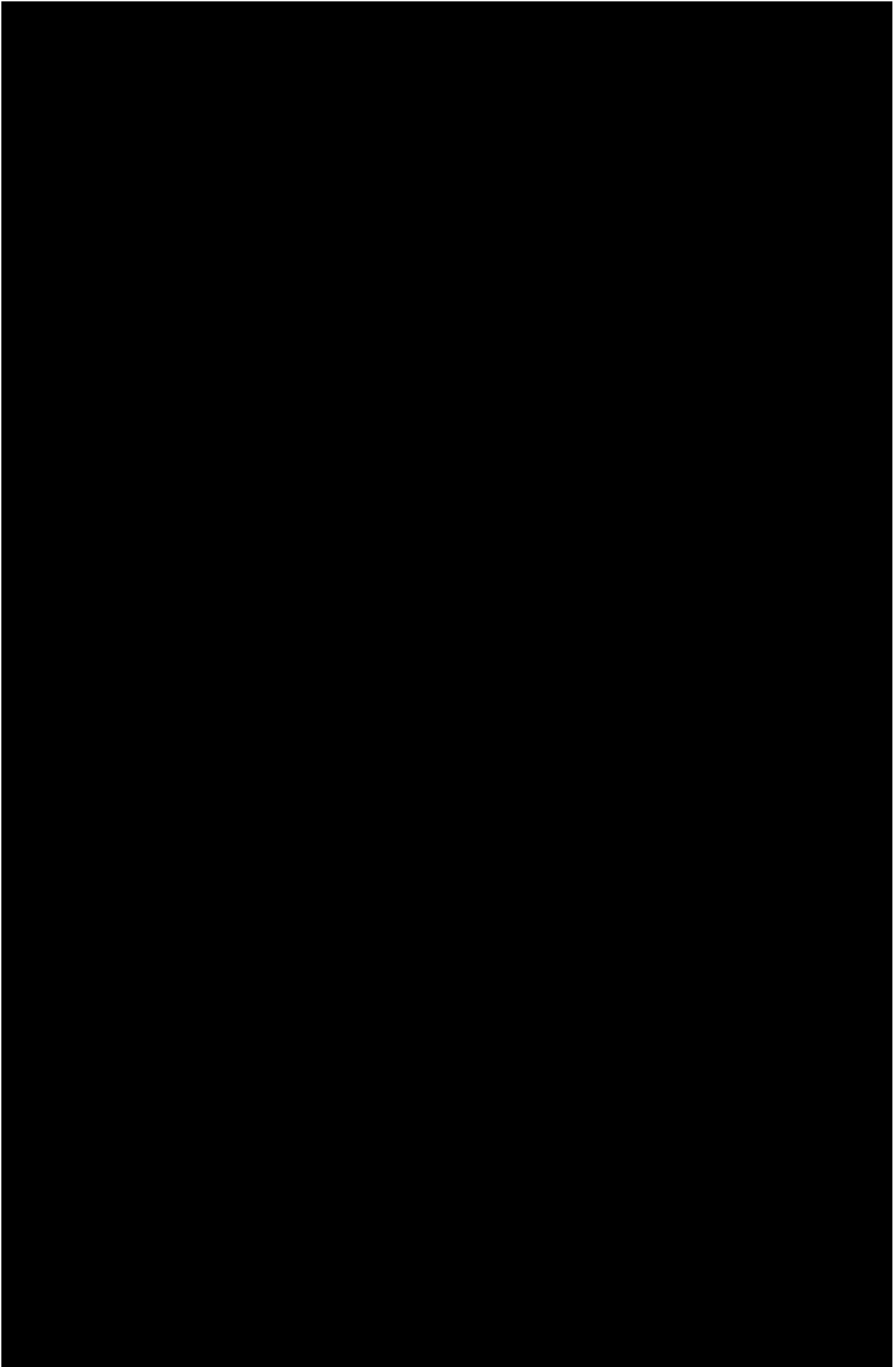
O&M Phase Payment Schedule

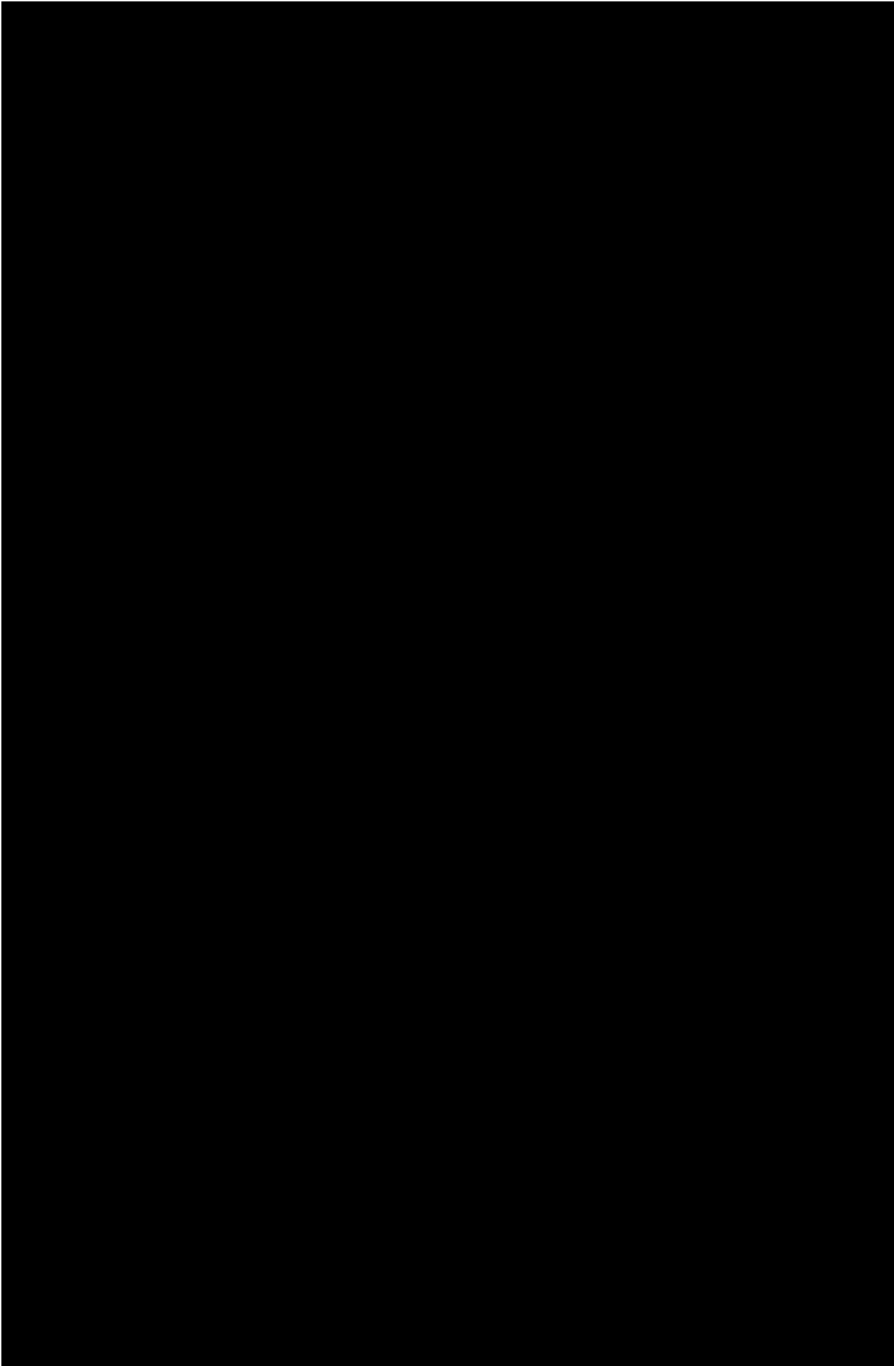
Item #	Project Execution Phase Deliverables	Estimated Invoice Month	Fees	Payment Amount
Year 2				
60	Monthly Operations & Maintenance Fee	Month 01	\$ 270,906	\$ 270,906
61	Monthly Operations & Maintenance Fee	Month 02	\$ 270,906	\$ 270,906
62	Monthly Operations & Maintenance Fee	Month 03	\$ 270,906	\$ 270,906
63	Monthly Operations & Maintenance Fee	Month 04	\$ 270,906	\$ 270,906
64	Monthly Operations & Maintenance Fee	Month 05	\$ 270,906	\$ 270,906
65	Monthly Operations & Maintenance Fee	Month 06	\$ 270,906	\$ 270,906
66	Monthly Operations & Maintenance Fee	Month 07	\$ 270,906	\$ 270,906
67	Monthly Operations & Maintenance Fee	Month 08	\$ 270,906	\$ 270,906
68	Monthly Operations & Maintenance Fee	Month 09	\$ 270,906	\$ 270,906
69	Monthly Operations & Maintenance Fee	Month 10	\$ 270,906	\$ 270,906
70	Monthly Operations & Maintenance Fee	Month 11	\$ 270,906	\$ 270,906
71	Monthly Operations & Maintenance Fee	Month 12	\$ 270,906	\$ 270,906
Total Year 2 O&M				\$ 3,250,869
Year 3				
72	Monthly Operations & Maintenance Fee	Month 01	\$ 264,683	\$ 264,683
73	Monthly Operations & Maintenance Fee	Month 02	\$ 264,683	\$ 264,683
74	Monthly Operations & Maintenance Fee	Month 03	\$ 264,683	\$ 264,683
75	Monthly Operations & Maintenance Fee	Month 04	\$ 264,683	\$ 264,683
76	Monthly Operations & Maintenance Fee	Month 05	\$ 264,683	\$ 264,683
77	Monthly Operations & Maintenance Fee	Month 06	\$ 264,683	\$ 264,683
78	Monthly Operations & Maintenance Fee	Month 07	\$ 264,683	\$ 264,683
79	Monthly Operations & Maintenance Fee	Month 08	\$ 264,683	\$ 264,683
80	Monthly Operations & Maintenance Fee	Month 09	\$ 264,683	\$ 264,683
81	Monthly Operations & Maintenance Fee	Month 10	\$ 264,683	\$ 264,683
82	Monthly Operations & Maintenance Fee	Month 11	\$ 264,683	\$ 264,683
83	Monthly Operations & Maintenance Fee	Month 12	\$ 264,683	\$ 264,683
Total Year 3 O&M				\$ 3,176,195
Year 4 - Optional				
84	Monthly Operations & Maintenance Fee	Month 01	\$ 247,221	\$ 247,221
85	Monthly Operations & Maintenance Fee	Month 02	\$ 247,221	\$ 247,221
86	Monthly Operations & Maintenance Fee	Month 03	\$ 247,221	\$ 247,221
87	Monthly Operations & Maintenance Fee	Month 04	\$ 247,221	\$ 247,221
88	Monthly Operations & Maintenance Fee	Month 05	\$ 247,221	\$ 247,221
89	Monthly Operations & Maintenance Fee	Month 06	\$ 247,221	\$ 247,221
90	Monthly Operations & Maintenance Fee	Month 07	\$ 247,221	\$ 247,221
91	Monthly Operations & Maintenance Fee	Month 08	\$ 247,221	\$ 247,221

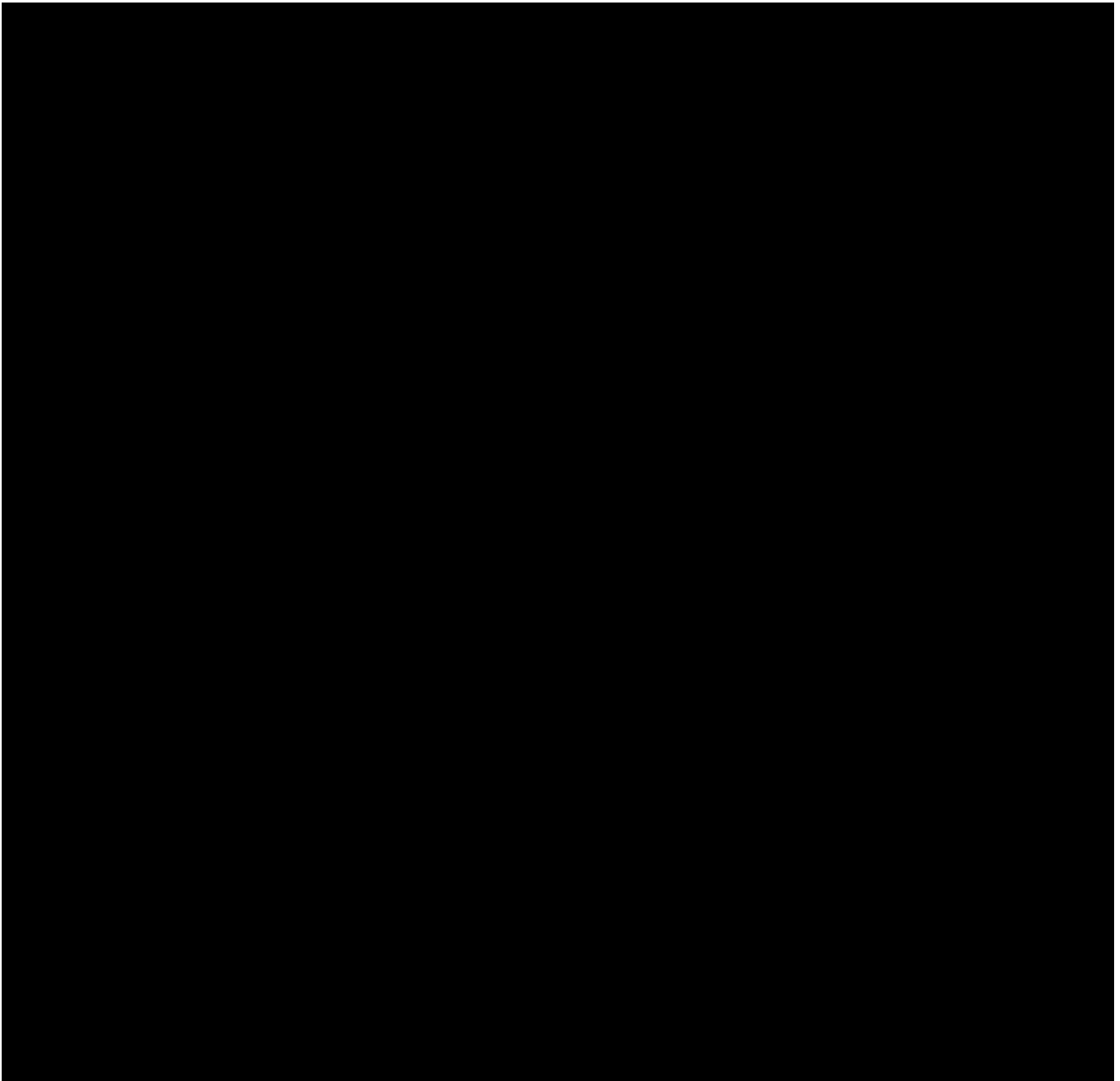
Item #	Project Execution Phase Deliverables	Estimated Invoice Month	Fees	Payment Amount
92	Monthly Operations & Maintenance Fee	Month 09	\$ 247,221	\$ 247,221
93	Monthly Operations & Maintenance Fee	Month 10	\$ 247,221	\$ 247,221
94	Monthly Operations & Maintenance Fee	Month 11	\$ 247,221	\$ 247,221
95	Monthly Operations & Maintenance Fee	Month 12	\$ 247,221	\$ 247,221
	Total Year 4 O&M			\$ 2,966,649
	Year 5 - Optional			
96	Monthly Operations & Maintenance Fee	Month 01	\$ 256,885	\$ 256,885
97	Monthly Operations & Maintenance Fee	Month 02	\$ 256,885	\$ 256,885
98	Monthly Operations & Maintenance Fee	Month 03	\$ 256,885	\$ 256,885
99	Monthly Operations & Maintenance Fee	Month 04	\$ 256,885	\$ 256,885
100	Monthly Operations & Maintenance Fee	Month 05	\$ 256,885	\$ 256,885
101	Monthly Operations & Maintenance Fee	Month 06	\$ 256,885	\$ 256,885
102	Monthly Operations & Maintenance Fee	Month 07	\$ 256,885	\$ 256,885
103	Monthly Operations & Maintenance Fee	Month 08	\$ 256,885	\$ 256,885
104	Monthly Operations & Maintenance Fee	Month 09	\$ 256,885	\$ 256,885
105	Monthly Operations & Maintenance Fee	Month 10	\$ 256,885	\$ 256,885
106	Monthly Operations & Maintenance Fee	Month 11	\$ 256,885	\$ 256,885
107	Monthly Operations & Maintenance Fee	Month 12	\$ 256,885	\$ 256,885
	Total Year 5 O&M			\$ 3,082,618

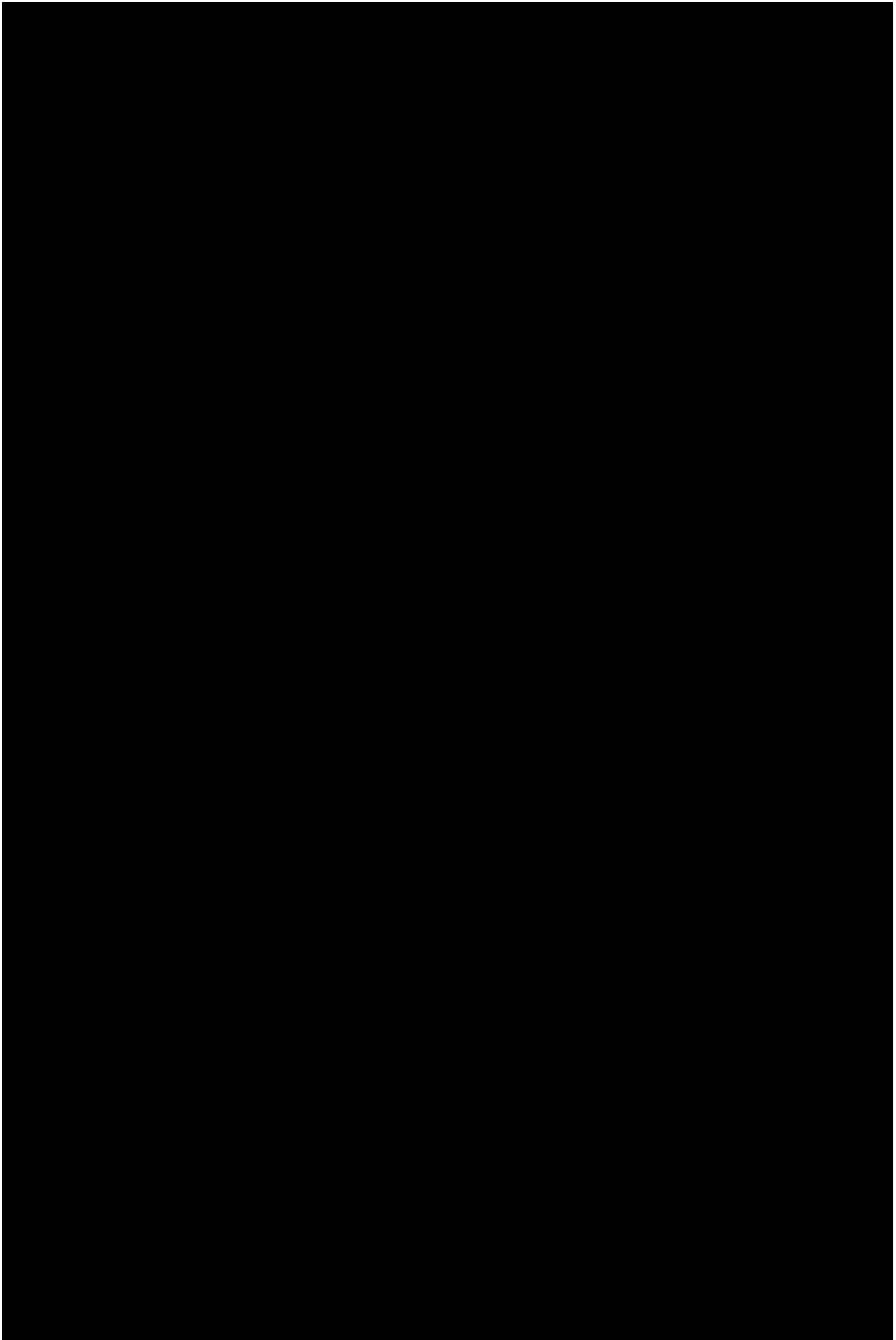
Dependencies and Conditions

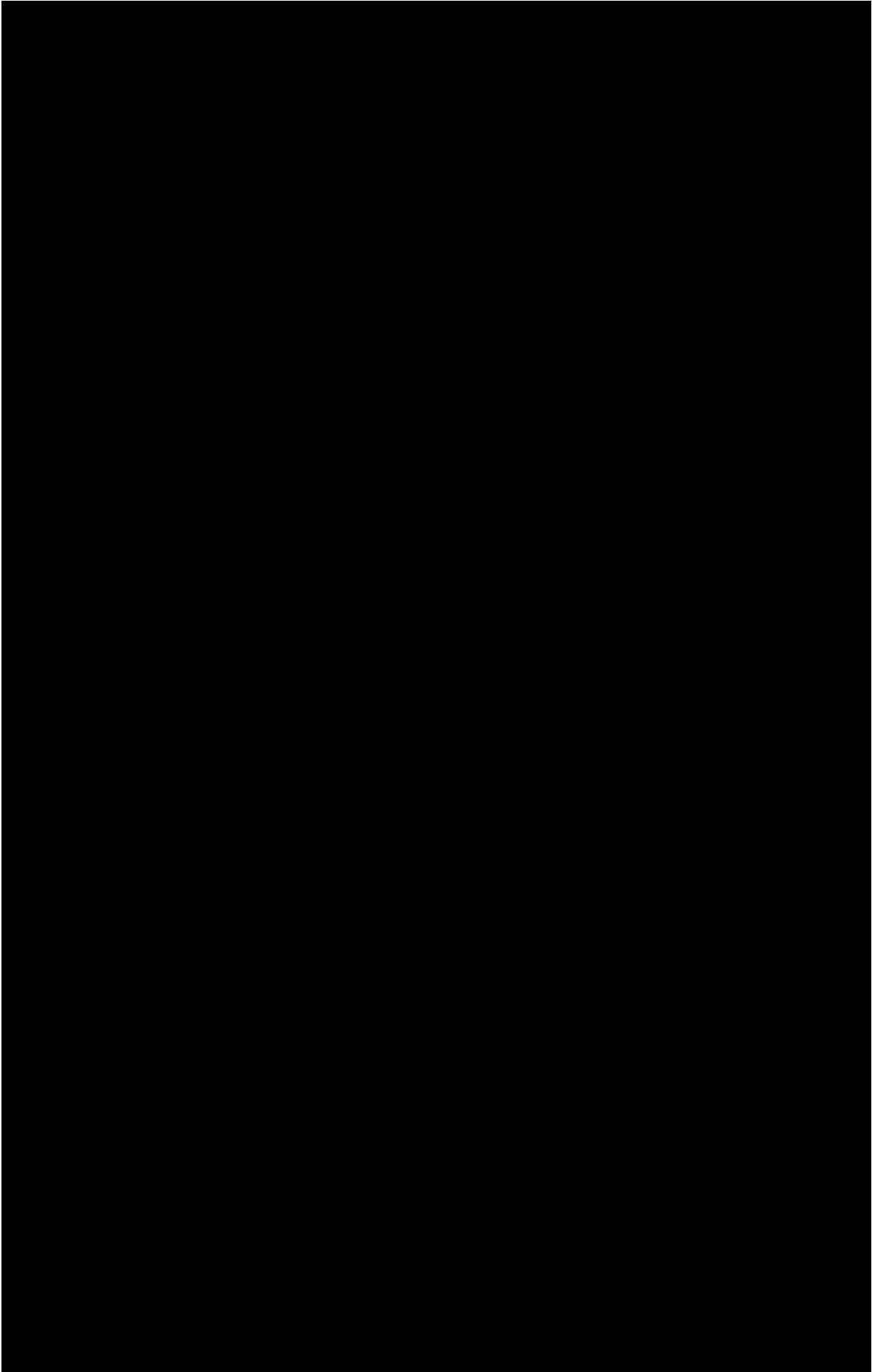


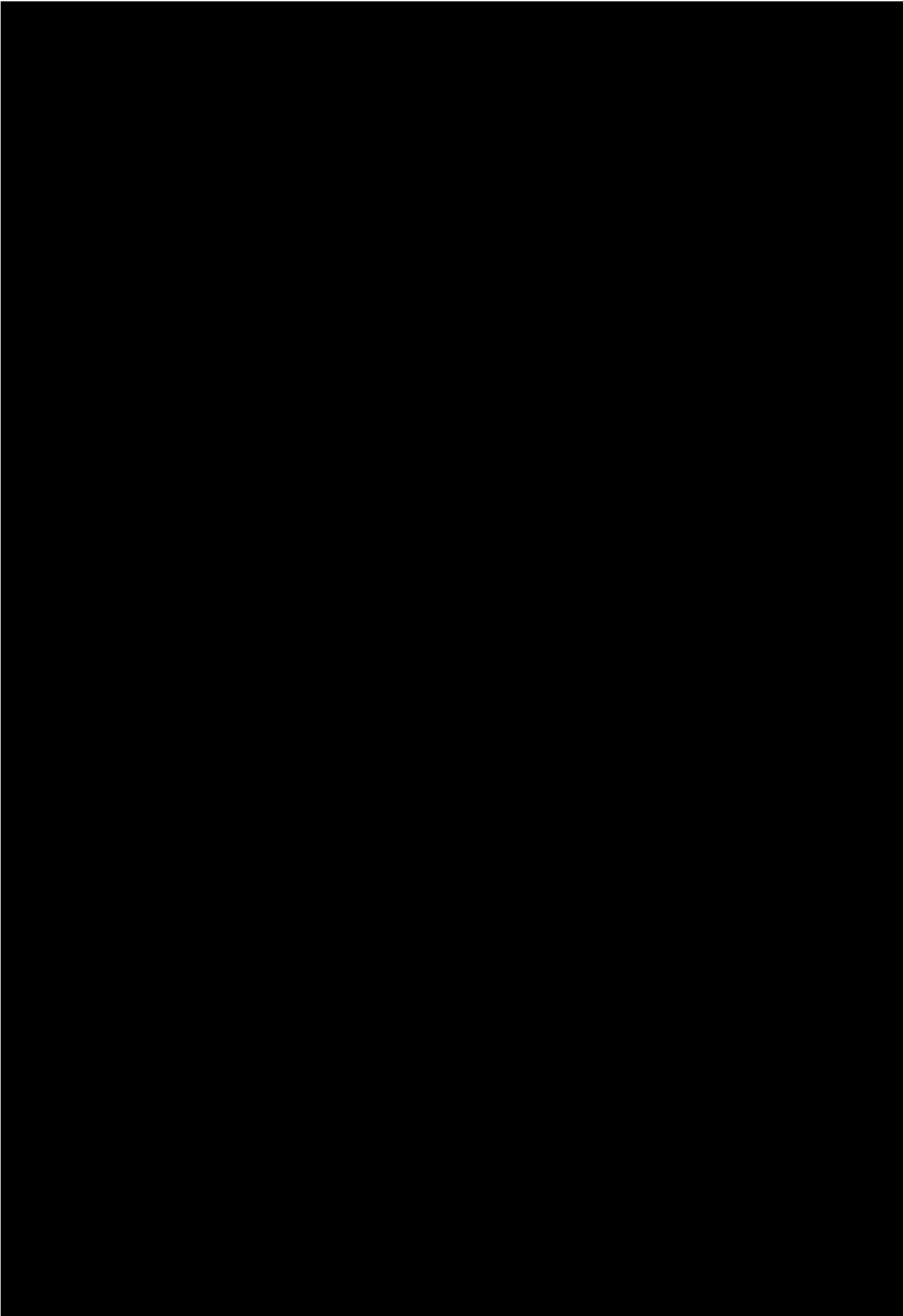


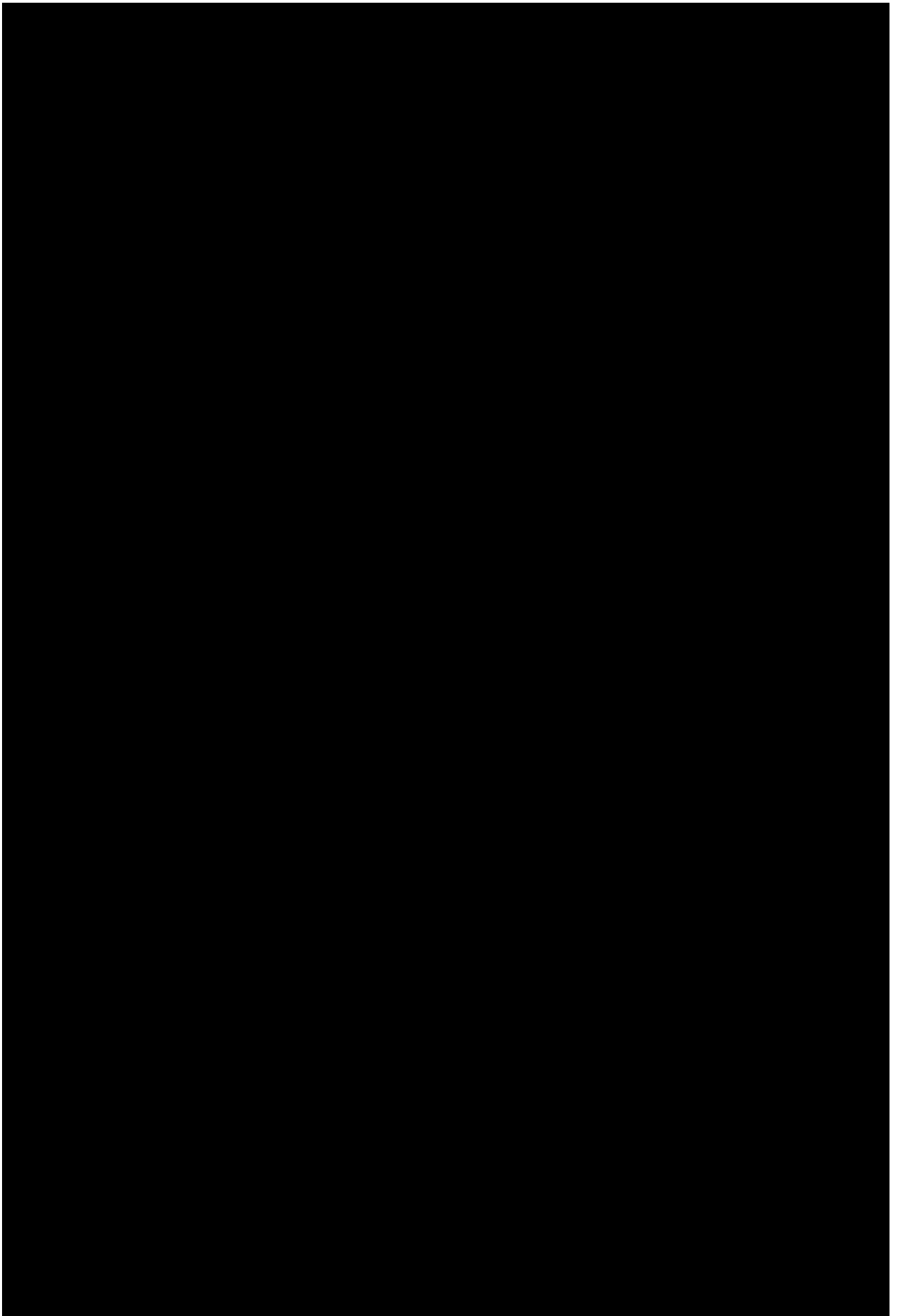


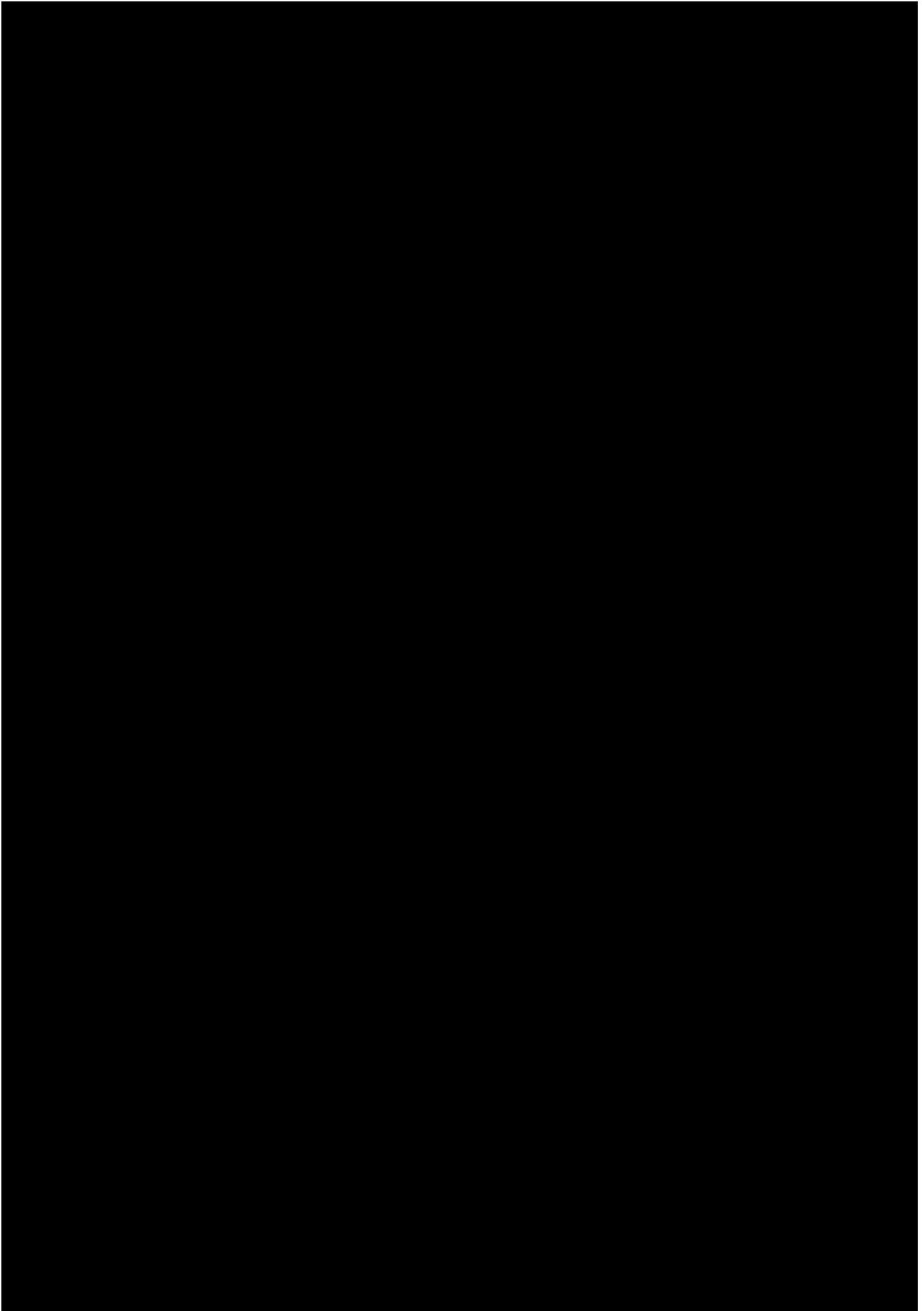


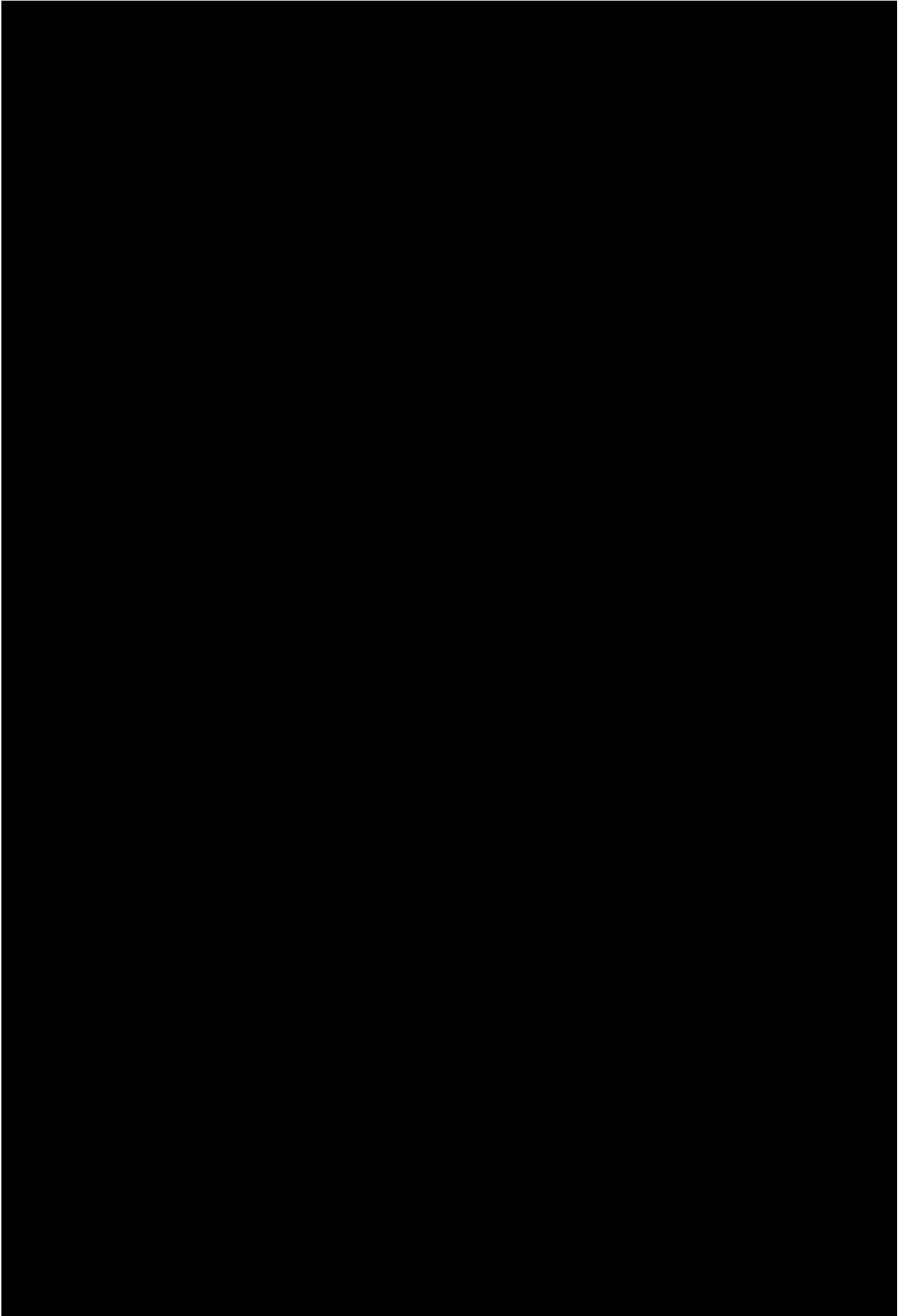












Software License Fees

The Vendor must list, itemize, and describe any applicable offer costs which may include the following
a) Software License fees or costs to accommodate user base identified.

We are pleased to present comprehensive quotes for the Salesforce and the DocuSign subscription costs, inclusive of terms and conditions, as provided by Carahsoft.

GOVERNMENT PRICE QUOTATION

SALESFORCE.COM GOVERNMENT at CARAHSOFT



CARAHSOFT TECHNOLOGY CORP.
11493 SUNSET HILLS ROAD | SUITE 100 | RESTON, VIRGINIA 20190
PHONE (703) 871-8500 | FAX (703) 871-8505 | TOLL FREE (888) 662-2724
www.carahsoft.com | sales@carahsoft.com

TO: Jillian Kennedy
Contract Specialist
NC Department of Health and Human Services
101 Blair Dr
Adams Building on Dorothea Dix Campus
Raleigh, NC 27603 USA

FROM: Peyton Stevens
Carahsoft Technology Corp.
11493 Sunset Hills Road
Suite 100
Reston, Virginia 20190

EMAIL: Jillian.kennedy@dhhs.nc.gov

EMAIL: Peyton.Stevens@carahsoft.com

PHONE:

PHONE: (571) 662-3388

FAX: (703) 871-8505

TERMS: FTIN: 52-2189693
Shipping Point: FOB Destination
Remit To: Same as Above
Payment Terms: Net 30 (On Approved Credit)
Cage Code: 1P3C5
DUNS No: 088365767
UEI: DT8KJHZXVJH5
Credit Cards: VISA/MasterCard/AMEX
Sales Tax May Apply

QUOTE NO: 40399452
QUOTE DATE: 08/09/2023
QUOTE EXPIRES: 09/08/2023
RFQ NO:
SHIPPING: ESD
TOTAL PRICE: \$445,005.78

TOTAL QUOTE: \$445,005.78

LINE NO.	PART NO.	DESCRIPTION	-	QUOTE PRICE	QTY	EXTENDED PRICE
----------	----------	-------------	---	-------------	-----	----------------

1	200013358	Public Sector Foundation - Unlimited Edition (Restricted Use) Start Date: 12/01/2023 End Date: 11/30/2024		\$501.10 OM	300	\$150,330.00
2	200013333	Customer Community for Public Sector - UE - Logins (Per Month) Start Date: 12/01/2023 End Date: 11/30/2024		\$0.9758 OM	40000	\$39,032.00
3	200005696	Salesforce Shield 30% of Net Price Includes 1 Intelligent Document Reader Start Date: 12/01/2023 End Date: 11/30/2024		\$47,007.69 OM	1	\$47,007.69
4	200013340	Customer Community Plus for Public Sector - UE - Members Start Date: 12/01/2023 End Date: 11/30/2024		\$7.5165 OM	16500	\$124,022.25
5	200000512	Sandbox (Full Copy) 30% of Net Price Start Date: 12/01/2023 End Date: 11/30/2024		\$47,007.69 OM	1	\$47,007.69
6	200000942	Government Cloud Plus 15% of Net Price Start Date: 12/01/2023 End Date: 11/30/2024		\$37,606.15 OM	1	\$37,606.15

SUBTOTAL: \$445,005.78

TOTAL PRICE: \$445,005.78

TOTAL QUOTE: \$445,005.78

GOVERNMENT PRICE QUOTATION

SALESFORCE.COM GOVERNMENT at CARAHSOFT



CARAHSOFT TECHNOLOGY CORP.

11493 SUNSET HILLS ROAD | SUITE 100 | RESTON, VIRGINIA 20190
PHONE (703) 871-8500 | FAX (703) 871-8505 | TOLL FREE (888) 662-2724
www.carahsoft.com | sales@carahsoft.com

LINE NO.	PART NO.	DESCRIPTION	-	QUOTE PRICE	QTY	EXTENDED PRICE
----------	----------	-------------	---	-------------	-----	----------------

****Please reference Carahsoft Quote # 40399061 on Purchase Order****

--- Quote Special Terms ---

Notwithstanding anything to the contrary to a Quote Special Term on this Order Form, "Reseller" means the entity signing this Order Form, and "Customer" means the entity to whom Reseller has resold the Services pursuant to the Reseller Agreement between Salesforce and Reseller ("Reseller Agreement"). Public Sector Foundation - Unlimited Edition (Restricted Use) subscriptions ordered hereunder at pricing of \$41.76/User/Month are Restricted Use Subscriptions, and shall be subject to the following restriction(s): Restricted Use Subscriptions shall (1) Exclude functionality for the following object(s): Assets, Employee Cases, Entitlements, Orders, Products, Price Books, Work Orders, Employee Work Orders, Authorizations, Volunteer Project, Volunteer Management, Action Plans; (2) Have access limited to 120 Custom Objects only; (3) Be accessed only by the following type(s) of user(s): NC Dept of Health and Human Services (NC DHHS) Division of Early Education and Child Development (DCDEE) workers; (4) Be access only for the following use case(s): State of North Carolina DHHS RFP NO. 30-23189 DCDEE – Workforce Registry and NC Pre-K and Regulatory System Replacement These restrictions shall be cumulative and shall apply to all Restricted Use Subscriptions purchased under this Order Form. Customer must strictly segregate all Restricted Use Subscriptions from any full-featured subscriptions it may hold by setting up and enforcing a unique profile in the Service associated with such Restricted Use Subscriptions. Customer understands that the above functionality limitations are contractual in nature (i.e., the functionality itself has not been disabled as a technical matter in the Service) and therefore agrees to strictly monitor its Users' use of such Restricted Use Subscriptions and enforce the applicable restrictions. Salesforce.com may audit Customer's use of Restricted Use Subscriptions at any time through the Service. Should any audit reveal any unauthorized use of Restricted Use Subscriptions, Customer agrees it will pay, within thirty (30) days of notice of the audit results, the difference between the contract price for Restricted Use Subscriptions and the list price for full subscriptions of the above-named product, for all of the Restricted Use Subscriptions showing unauthorized use (taken as a group), beginning with the date of the first violation through the end of the then current subscription term. Upon such payment, all such Restricted Use Subscriptions showing unauthorized use will be converted into full subscriptions for the remainder of the then current subscription term.

For the first renewal term, provided that (a) Customer renews its entire subscription volume under this Order Form combined with any associated add-on Order Forms, and (b) the renewal term is for one year, pricing and minimum quantities (as increased by any add-on orders) shall be as stated below. For the avoidance of doubt, the quantities stated below shall be increased by any add-on orders during the term of this Order Form. 300 Public Sector Foundation - Unlimited Edition (Restricted Use) for \$73.10 user/month; 40,000 Customer Community for Public Sector - UE - Logins (Per Month) for \$0.13 user/month; 16,500 Customer Community Plus for Public Sector - UE - Members for \$1.09 user/month; 1 Government Cloud Plus for 12% of net; 1 Salesforce Shield for 15% of net sales; and 1 Sandbox (Full Copy) for 15% of net sales. For the second renewal term, provided that (a) Customer renews its entire subscription volume under this Order Form combined with any associated add-on Order Forms, and (b) the renewal term is for one year, pricing and minimum quantities (as increased by any add-on orders) shall be as stated below. For the avoidance of doubt, the quantities stated below shall be increased by any add-on orders during the term of this Order Form or during the first renewal term. 300 Public Sector Foundation - Unlimited Edition (Restricted Use) for \$104.40 user/month; 40,000 Customer Community for Public Sector - UE - Logins (Per Month) for \$0.20 user/month; 16,500 Customer Community Plus for Public Sector - UE - Members for \$1.56 user/month; 1 Government Cloud Plus for 12% of net sales; 1 Salesforce Shield for 15% of net sales; and 1 Sandbox (Full Copy) for 15% of net sales. For the third and fourth renewal terms, provided (a) Customer renews its entire subscription volume under this Order Form combined with any associated add-on Order Forms (including any subscriptions added during the renewal terms), and (b) each renewal term is for one year, any increase in subscription pricing (excluding support and resource-based Services) for the third and fourth renewal terms will not exceed 3% over the then-current subscription pricing. Thereafter, or upon a renewal that does not meet the aforementioned criteria for Customer to benefit from the above price cap, any increase in subscription and support pricing will be in accordance with pricing and policies in effect at the time of the renewal or as otherwise agreed to by the parties. SFDC shall use reasonable efforts to ensure that the pricing offered in any subsequent Order Form reflects the pricing offered to Customer in this quote specific term. However, Customer is responsible for confirming the accuracy of such pricing prior to signing any subsequent Order Form. In the event of a conflict between the pricing indicated here and that included in any new Order Form, the pricing in the new Order Form shall control as to the subscriptions purchased in that new Order Form.

Notwithstanding anything to the contrary, subscriptions purchased pursuant to this Order Form shall not automatically renew, and therefore shall terminate on the applicable Order End Date above unless Customer enters into a new Order Form with Salesforce, on or before that Order End Date, for the relevant product(s).

Only Services on this Order Form that are identified by SKU in the Government Cloud Plus Products list available at <https://www.salesforce.com/company/legal/agreements/>, as updated from time to time, are Government Cloud Plus Products. All other Services are non-Government Cloud Plus products. The Government Cloud Available Products and Features Knowledge Article available at <https://help.salesforce.com/articleView?id=000321821&type=1&mode=1> ("Knowledge Article") identifies "Interoperable (but not authorized)" products and features which are compatible with Government Cloud Plus Products, in the manner as described in the Documentation. Customer has sole responsibility, prior to using new products or features with Government Cloud Plus Products, to determine if such products or features are within the Government Cloud Plus authorization boundary, as described in the Knowledge Article, and for maintaining the settings in its Salesforce Government Cloud Plus Org for the Org to remain compliant with the Government Cloud Plus authorizations. Salesforce provides customers with a Configuration User Guide available at <https://publicsector-compliance-us.my.salesforce.com/> to assist with the setup and configuration process. "Org" means a unique instance of the Services, i.e., a separate set of Customer Data and Customer-specific Service customizations held by SFDC in a logically separated database (i.e., a database segregated through password-controlled access). Customer acknowledges that the "Interoperable (but not authorized)" products and features, as well as any Non-SFDC Applications that interoperate with the Customer's Salesforce Government Cloud Plus Org, fall outside of the Government Cloud Plus authorization boundary. In light of the foregoing, Customer understands and agrees that

GOVERNMENT PRICE QUOTATION

SALESFORCE.COM GOVERNMENT at CARAHSOFT



CARAHSOFT TECHNOLOGY CORP.

11493 SUNSET HILLS ROAD | SUITE 100 | RESTON, VIRGINIA 20190
PHONE (703) 871-8500 | FAX (703) 871-8505 | TOLL FREE (888) 662-2724
www.carahsoft.com | sales@carahsoft.com

LINE NO.	PART NO.	DESCRIPTION	-	QUOTE PRICE	QTY	EXTENDED PRICE
----------	----------	-------------	---	-------------	-----	----------------

its Customer Data will be shared with "Interoperable (but not yet authorized)" products and features and Non-SFDC Applications that interoperate with its Salesforce Government Cloud Plus Org.

--- Product Special Terms ---

INFORMATION SHARING - AWS

Customer consents to SFDC sharing with AWS information about Customer's purchase of Services that interoperate with AWS services and functionality, including but not limited to Customer name, order details, address, Customer's AWS ID(s), account and opportunity information, and contact information. Customer agrees that AWS' collection, use, storage, processing and handling of such information, together with relevant portions of this Order Form as referenced below, once received by AWS, is governed by the agreement between AWS and Customer as though Customer or its Users provided it directly to AWS. By signing this Order Form, Customer agrees, as a direct obligation to Amazon Web Services, Inc. or its affiliates (defined as any relevant affiliate or group company of Amazon, as may be updated by Amazon from time to time) ("AWS"), that AWS may share information about Customer's use of AWS services with Salesforce for product collaboration, accounting, customer support, troubleshooting, and product review purposes, and AWS may share relevant portions of this Order Form, as provided to AWS by Salesforce, with applicable governmental agencies and adjudicative bodies to prove that Customer provided consent to share this information with Salesforce.

Einstein Features

SFDC may access Customer Data submitted to the Einstein features for the purpose of improving and training services and features Customer may access, and Customer instructs SFDC to process its Customer Data for such purpose. Customer retains all ownership of its Customer Data and SFDC retains all ownership in and to aggregated machine learning results.

Government Cloud Plus

The Government Cloud Plus subscription: (i) provides an isolated infrastructure for hosting authorized Salesforce Services, with additional controls specifically for US government customers and US government contractors, as further described in the Trust and Compliance Documentation (available at <https://www.salesforce.com/company/legal/trust-and-compliance-documentation/>); and (ii) amends and supplements the Premier Success Plan (available at <https://sfdc.co/bDsV6q>) for Services available on the Government Cloud Plus infrastructure as set forth below. The terms in the Premier Success Plan shall apply, except as otherwise set forth herein. For the purposes of this Product Special Term, "Qualified US Citizens" are individuals who: (1) are United States citizens; (2) are physically located within the United States while providing Premier Support Services; and (3) have completed a background check as a condition of their employment with Salesforce. Submitting a Case: Users can submit support cases as described in the Premier Success Plan. Cases submitted via the Help portal will automatically be routed to Qualified US Citizens. Cases submitted outside of the Help portal (e.g. via telephone or chat, when available) will not be responded to by Qualified US Citizens. These individuals will route cases to a team of Qualified US Citizens and will access the following information about Users in order to route the calls to Qualified US Citizens: first and last name, email address, username, phone number, and physical business address. All support is provided in English only. All personnel engaged outside of the Help portal, including those in customer success roles or providing customer success services (e.g. Expert Coaching, Expert Office Hours), will not be Qualified US Citizens and will only have access to Customer Data if Customer provides such personnel a User ID or otherwise enables the sharing of Customer Data with such personnel.

Emergency Program Management

In order to access Emergency Program Management Services, Customer's system administrator must first install the managed package via the following link: <http://industries.force.com/publicsector>.

Public Sector Foundation

In order to access Omnistudio features and functionality, Customer's system administrator must first install the latest OmniStudio managed package available at: <https://docs.vlocity.com/en/Omnistudio-Release-Summary.html>. Customer must be using a version of the managed package that is no more than two releases behind the then-current generally available version of the managed package (the "GA Version") in order for SFDC to provide support. SFDC will not provide support for Omnistudio features and functionality to Customer (including any patches) for any managed package that is more than two releases behind the GA Version.

Salesforce Shield

In order to use the Data Detect features, Customer's system administrator must first install the managed package available at: <https://sfdc.co/install-datadetect>. Customer must reference Quote number and Contract # on Purchase Order.

Should Customer purchase via Reseller all terms of Carahsoft Quote must be incorporated in Reseller quote and Customer Purchase Order to Reseller.

Any increase in subscription pricing (excluding support and resource-based Services) for the first renewal term will not exceed 5% over the then-current subscription pricing, provided that (a) Customer renews its entire then-current subscription volume under this Order Form combined with any associated add-on Order Forms, and (b) the first renewal term is the same duration as the Order Term of this Order Form or one year (whichever is longer). Thereafter, any increase in subscription and support pricing will be in accordance with SFDC's pricing and policies in effect at the time of the renewal or as otherwise agreed to by the parties

Licensee agrees that any order for Salesforce Services will be governed by the terms and conditions of the Carahsoft Salesforce Service Terms, copies of which are found at <https://carah.io/SFDC-TOU> and all Schedules and Documentation referenced by the Terms are made a part hereof. The parties agree that any term or condition stated in a Customer purchase order or in any other Customer order documentation (excluding Quotes) is void. In the event of any conflict or inconsistency among the following documents, the order of precedence shall be: (1) the applicable Quotes (and their Contract Vehicle), (2) the TOU, and (3) the Documentation. Licensee

GOVERNMENT PRICE QUOTATION



SALESFORCE.COM GOVERNMENT at CARAHSOFT



CARAHSOFT TECHNOLOGY CORP.
11493 SUNSET HILLS ROAD | SUITE 100 | RESTON, VIRGINIA 20190
PHONE (703) 871-8500 | FAX (703) 871-8505 | TOLL FREE (888) 662-2724
www.carahsoft.com | sales@carahsoft.com

LINE NO.	PART NO.	DESCRIPTION	-	QUOTE PRICE	QTY	EXTENDED PRICE
----------	----------	-------------	---	-------------	-----	----------------

acknowledges it has had the opportunity to review the Terms, prior to executing an order.

Product Terms Directory: <http://carah.io/Product-Terms-Directory>
Help & Training: <http://carah.io/Help>
Government Cloud Plus: <http://www.carahsoft.com/government-cloud-terms>

A list of currently available FedRAMP/IL4 Authorized Salesforce products can be found here:
https://help.salesforce.com/articleView?id=000270080&language=en_US&type=1

Government - Price Quotation



DocuSign Government at Carahsoft



11493 Sunset Hills Road | Suite 100 | Reston, Virginia 20190
Phone (703) 871-8500 | Fax (703) 871-8505 | Toll Free (888) 662-2724
www.carahsoft.com | sales@carahsoft.com

TO: Accenture 800 N Glebe Rd Suite 300 Arlington, VA 22203	FOR: Pamela Jackson Administrative Officer DHHS Raleigh, NC 27609	FROM: Grace Ferrara DocuSign Government at Carahsoft 11493 Sunset Hills Road Suite 100 Reston, Virginia 20190
EMAIL:	EMAIL: pamela.jackson@dhhs.nc.gov	EMAIL: Grace.Ferrara@carahsoft.com
PHONE:	PHONE:	PHONE: (571) 662-3412
		FAX: (703) 871-8505

TERMS: FTIN: 52-2189693
Shipping Point: FOB Destination
Remit To: Same as Above
Payment Terms: Net 30 (On Approved Credit)
Cage Code: 1P3C5
DUNS No: 088365767
UEI: DT8KJHZXVJH5
Credit Cards: VISA/MasterCard/AMEX
Credit Card Fees May Apply
Sales Tax May Apply

QUOTE NO: 40489912
QUOTE DATE: 08/15/2023
QUOTE EXPIRES: 08/31/2023
RFQ NO:
SHIPPING: ESD
TOTAL PRICE: \$73,876.74

TOTAL QUOTE: \$73,876.74

LINE NO.	PART NO.	DESCRIPTION	-	QUOTE PRICE	QTY	EXTENDED PRICE
1	APT-0210-2	DocuSign Connector - Salesforce Per Seat Annual DocuSign, Inc. - APT-0210		\$0.00 OM	155500	\$0.00
2	APT-0148-2	Enterprise Premier Support 22% of Recurring Fees (22% of List Price per \$100 of List License Fees) DocuSign, Inc. - APT-0148		\$13,309.49 OM	1	\$13,309.49
3	APT-0395-2	DocuSign Enterprise Pro for Gov - Env (Adopt. Accel.) DocuSign, Inc. - APT-0395		\$0.3895 OM	155500	\$60,567.25
SUBTOTAL:						\$73,876.74
TOTAL PRICE:						\$73,876.74
TOTAL QUOTE:						\$73,876.74



11493 Sunset Hills Road | Suite 100 | Reston, Virginia 20190
 Phone (703) 871-8500 | Fax (703) 871-8505 | Toll Free (888) 662-2724
 www.carahsoft.com | sales@carahsoft.com

LINE NO.	PART NO.	DESCRIPTION	-	QUOTE PRICE	QTY	EXTENDED PRICE
----------	----------	-------------	---	-------------	-----	----------------

Product Details
 eSignature Envelope Allowance: 155,500

Order Special Terms

For the Adoption Accelerator package(s) purchased in this Order Form, for the duration of the contract Term, no overage charges shall apply for reasonable use of the Subscription Services, not exceeding 150% of the specified Envelope Allowance ("Reasonable Use"). Usage is limited to a single use case, to a single site ID, and is non-transferable in the event that Customer acquires an entity or is acquired. For the avoidance of doubt, the Adoption Accelerator package is not renewable.

Prior to overages and before August 12, 2024, Customer will have the option to purchase additional Envelopes, in minimum bundles of 10,000 Envelopes, at the same per-Envelope rate described in this Order Form, defined as \$0.37 per-Envelope, exclusive of Support, for use during the remainder of the Term.

If Customer elects to renew its subscription with DocuSign for the same length of Term as described in this Order Form, DocuSign agrees that the price for such subscription will not increase more than 5% over the previous Term for the same type eSignature Enterprise Pro for Gov Envelopes, DocuSign Connector - Salesforce, estimated Envelope Allowance and quantity of subscription(s) as described in this Order Form. This offer applies to one 12 month renewal only (Year 2) and does not apply to any third-party products, Professional Services or new products not included in this original Order Form.

If Customer elects to renew its subscription with DocuSign for the same length of Term as described in this Order Form, DocuSign agrees that the price for such subscription will not increase more than 7% over the previous Term for the same type eSignature Enterprise Pro for Gov Envelopes, DocuSign Connector - Salesforce, estimated Envelope Allowance and quantity of subscription(s) as described in this Order Form. This offer applies to three 12 month renewals only (Years 3, 4, and 5) and does not apply to any third-party products, Professional Services or new products not included in this original Order Form.

The eSignature Enterprise Pro for Gov Envelope sold at \$0.37 per envelope, exclusive of Support, is a restricted use subscription and contains the following limitations and/or restrictions: Customer may only access Signature Enterprise Pro for Salesforce Envelope, located in North Carolina, USA, for the following use case: NC DHHS Pre-K Program. These limitations are cumulative and contractual in nature. Customer agrees to keep these restricted use subscriptions in a unique instance of DocuSign and not co-mingle restricted use subscriptions with full use subscriptions. DocuSign, Inc. reserves the right to audit Customer's usage of all of its subscriptions. If at any time an audit reveals that Customer's use of any restricted use subscription is in violation of these terms, then the restricted use subscription(s) will immediately be converted into full use subscriptions at the then-current list price. Customer will be invoiced from the date of the first violation for the difference between the price of the limited use subscriptions and the full-use list price, and payment will be due per the terms of the Agreement.

Customer must reference Quote number on Purchase Order.

Should Customer purchase via Reseller all terms of Carahsoft Quote must be incorporated in Reseller quote and Customer Purchase Order to Reseller.

Any increase in subscription and support pricing will be in accordance with DocuSign's pricing and policies in effect at the time of the renewal or as otherwise agreed to by the parties.

Licensee agrees that any order for DocuSign will be governed by the terms and conditions of the Carahsoft DocuSign Service Agreement copies of which are found at https://static.carahsoft.com/concrete/files/2616/5962/5258/DocuSign_Master_Services_Agreement_fo_Public_Sector.pdf and all Schedules and Documentation referenced by the Terms are made a part hereof. The parties agree that any term or condition stated in a Customer purchase order or in any other Customer order documentation (excluding Quotes) is void. In the event of any conflict or inconsistency among the following documents, the order of precedence shall be: (1) the applicable Quotes (and their Contract Vehicle), (2) the TOU, and (3) the Documentation. Licensee acknowledges it has had the opportunity to review the Terms, prior to executing an order.

Should the customer purchase any version of DocuSign's IL-4 licensing the below terms will apply.

Reference the Memorandum previously provided to DISA Authorizing Official (dated March 27, 2021) detailing the Provisional Authorization (PA) granted by DISA, exceptions to/exclusions from the PA, and conditions DocuSign is required to meet in order to maintain the PA.

DocuSign is not yet authorized to connect to NIPRnet. Customer acknowledges that as of the Order Start Date, DocuSign does not have a BCAP connection to NIPRnet. Therefore, as a result, if Customer does not currently have DISA approval to forego the BCAP connection to NIPRnet:

- Customer will not use any DocuSign DoD/IL-4 products in production without a BCAP connection (or DISA approval);
 - Customer will not host, store or transmit production data in the IL4 environment without a BCAP connection to NIPRnet or a documented exception from DISA per to use DocuSign products while forgoing the BCAP;
 - Customer agrees not to use any DocuSign DoD/IL-4 products to connect to any DocuSign environment via a non BCAP end point without a documented exception from DISA to use DocuSign products while forgoing the BCAP;
 - Customer is responsible for any customer data sent to third party applications (regardless of whether third party applications are IL-4 certified).
- Enterprise Premier Support for IL-4 customers is available from 9:00am - 8:30pm Eastern Standard Time.



Section h)

Schedule of Offered Solution

h) Schedule of Offered Solution

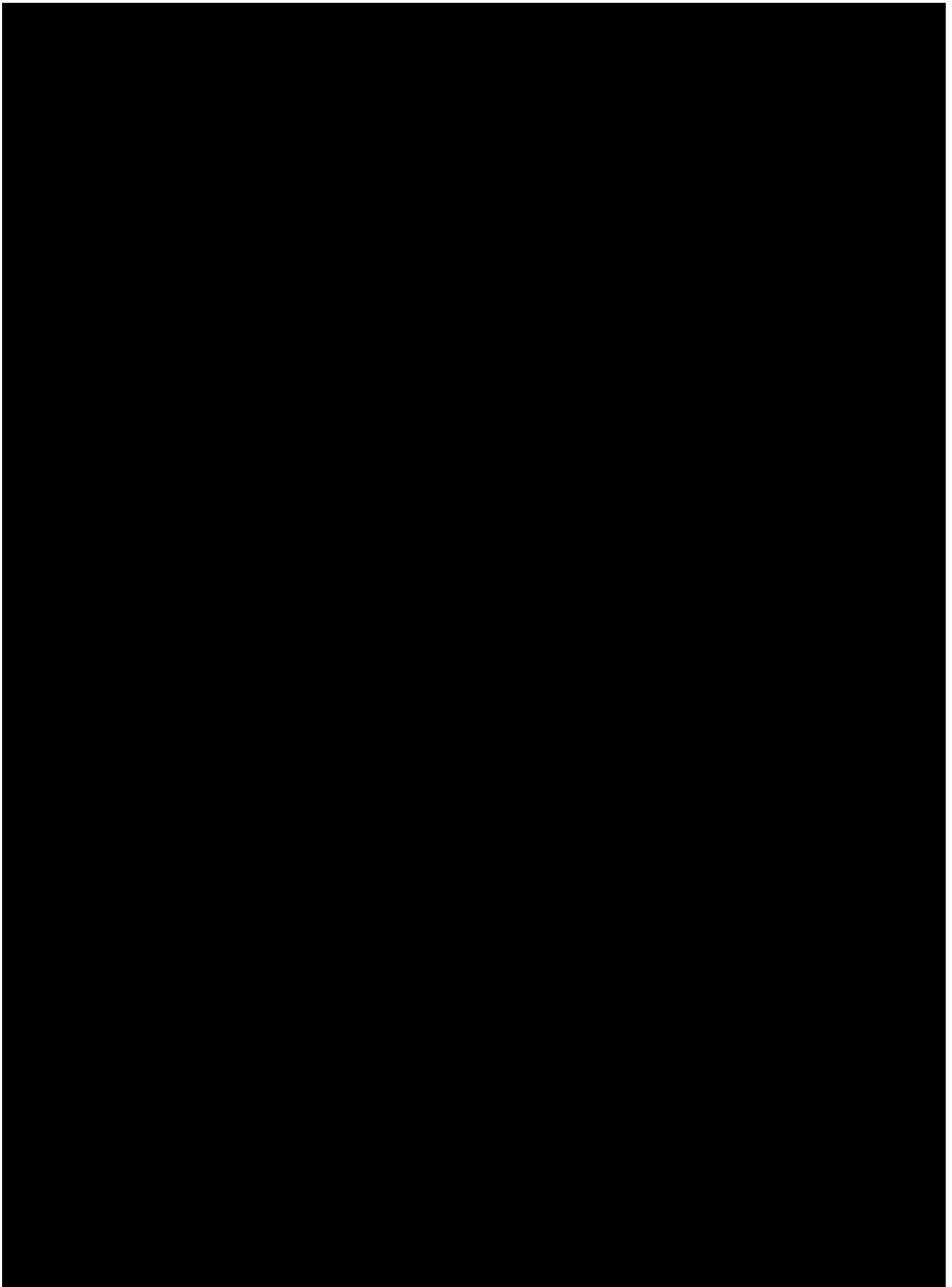
Delivery Provision: Draft submitted as part of the Vendor Proposal and reviewed with Agency within fifteen (15) days of Contract award. Final schedule due within twenty (20) State Business Days of the Contract award. Schedule Baseline is due once the Agency accepts the final Vendor Project Schedule. Project Execution Contract Phase Duration, updated weekly two (2) days prior to next scheduled Project Status Meeting; and ad hoc as requested by the Agency.

Purpose/Description: The Vendor Project Schedule defines all the tasks necessary for the Vendor proposed project delivery method, associated interdependencies, and task resource assignments to execute the project.

Vendor Project Schedule will: be developed with Microsoft Project™ or a Microsoft Project compatible product.

Minimum Content:

- Clearly map to the State's and NCDHHS's Project Management Stages, and Sprint Cycles/Modules/Milestones and Deliverables outlined in this RFP;
 - Sub-divide all tasks until no more than eighty (80) hours are allocated to each task;
 - Identify each Sprint Cycles/Modules/Milestones/ Deliverables cycle
 - Identify capability/functionality developed by the Sprint Cycles/Modules/Milestones/ Deliverables
 - The expected duration of the Sprint Cycles/Modules/Milestones/ Deliverables
 - The order of the Sprint Cycles/Modules/Milestones/ Deliverables
 - Projected task start and end dates;
 - Major business decision points and Deliverables defined in this RFP;
 - Projected Sprint Cycles/Modules/Milestones/decision point due dates;
 - Task dependencies;
-





Section i)

Signed Vendor Certification Form (Attachment F)

i) Signed vendor certification form (Attachment F)

ATTACHMENT F: VENDOR CERTIFICATION FORM

1) ELIGIBLE VENDOR

The Vendor certifies that in accordance with N.C.G.S. §143-59.1(b), Vendor is not an ineligible vendor as set forth in N.C.G.S. §143-59.1 (a).

The Vendor acknowledges that, to the extent the awarded contract involves the creation, research, investigation or generation of a future RFP or other solicitation; the Vendor will be precluded from bidding on the subsequent RFP or other solicitation and from serving as a subcontractor to an awarded vendor.

The State reserves the right to disqualify any bidder if the State determines that the bidder has used its position (whether as an incumbent Vendor, or as a subcontractor hired to assist with the RFP development, or as a Vendor offering free assistance) to gain a competitive advantage on the RFP or other solicitation.

2) CONFLICT OF INTEREST

Applicable standards may include: N.C.G.S. §§143B-1352 and 143B-1353, 14-234, and 133-32. The Vendor shall not knowingly employ, during the period of the Agreement, nor in the preparation of any response to this solicitation, any personnel who are, or have been, employed by a Vendor also in the employ of the State and who are providing Services involving, or similar to, the scope and nature of this solicitation or the resulting contract.

3) E-VERIFY

Pursuant to N.C.G.S. § 143B-1350(k), the State shall not enter into a contract unless the awarded Vendor and each of its subcontractors comply with the E-Verify requirements of N.C.G.S. Chapter 64, Article 2. Vendors are directed to review the foregoing laws. Vendors claiming exceptions or exclusions under Chapter 64 must identify the legal basis for such claims and certify compliance with federal law regarding registration of aliens including 8 USC 1373 and 8 USC 1324a. Any awarded Vendor must submit a certification of compliance with E-Verify to the awarding agency, and on a periodic basis thereafter as may be required by the State.

4) CERTIFICATE TO TRANSACT BUSINESS IN NORTH CAROLINA

As a condition of contract award, awarded Vendor shall have registered its business with the North Carolina Secretary of State and shall maintain such registration throughout the term of the Contract.

Signature: _____  _____

Date: 8/17/2023

Printed Name: ___Natalie Batten_____ Title: Managing Director



Section j)

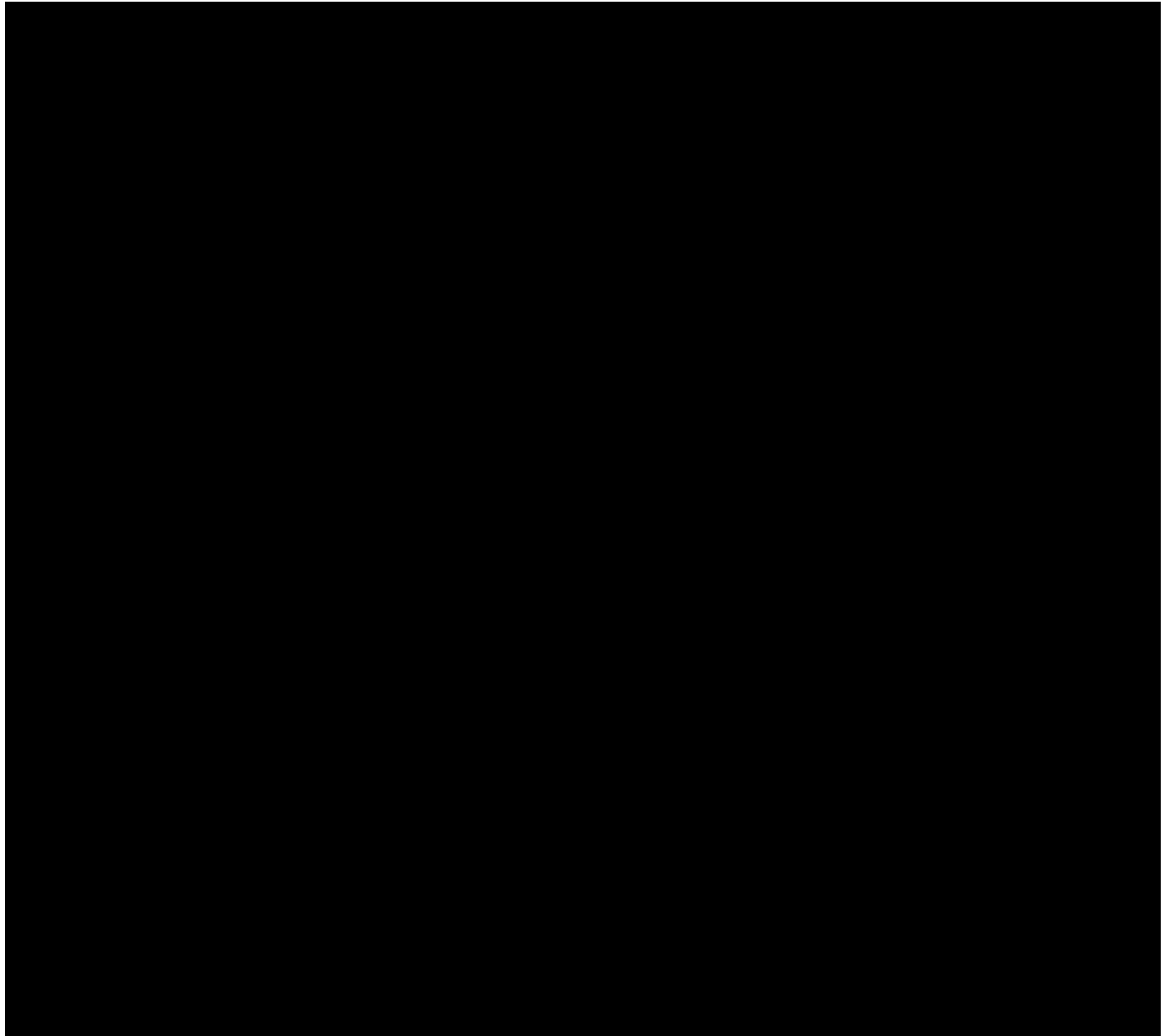
Location of Workers Utilized by Agency (Attachment G)

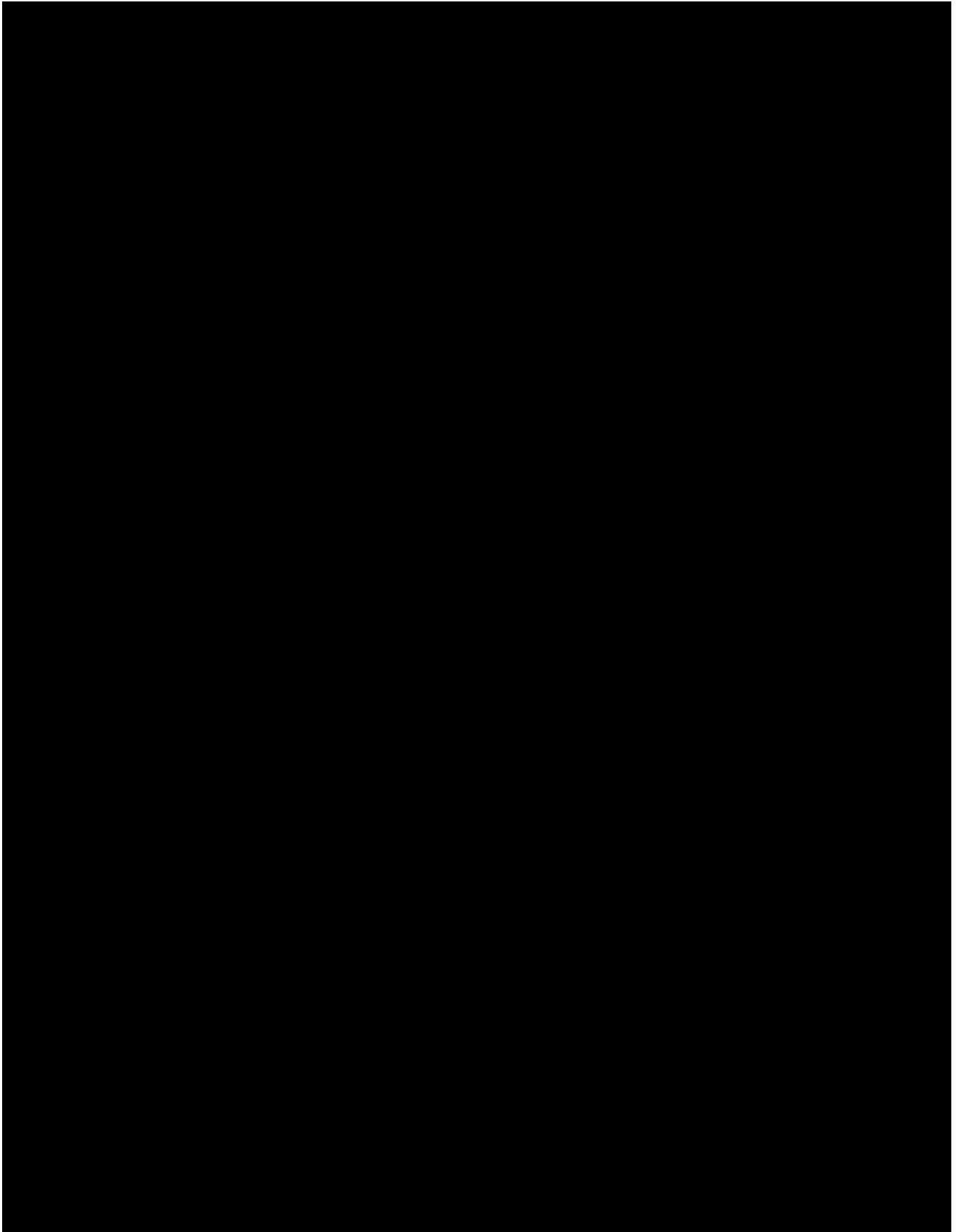
j) Location of Workers Utilized by Agency (Attachment G)

In accordance with N.C.G.S. §143B-1361(b), Vendor must identify how it intends to utilize resources or workers located outside the U.S., and the countries or cities where such are located. The State will evaluate additional risks, costs, and other factors associated with the Vendor's utilization of resources or workers prior to making an award for any such Vendor's offer. The Vendor shall provide the following:

1) The location of work to be performed by the Vendor's employees, subcontractors, or other persons, and whether any work will be performed outside the United States. The Vendor shall provide notice of any changes in such work locations if the changes result in performing work outside of the United States.

2) Any Vendor or subcontractor providing support or maintenance Services for software, call or contact center Services shall disclose the location from which the call or contact center Services are being provided upon request.







Section k)

References

k) References

ATTACHMENT H: REFERENCES

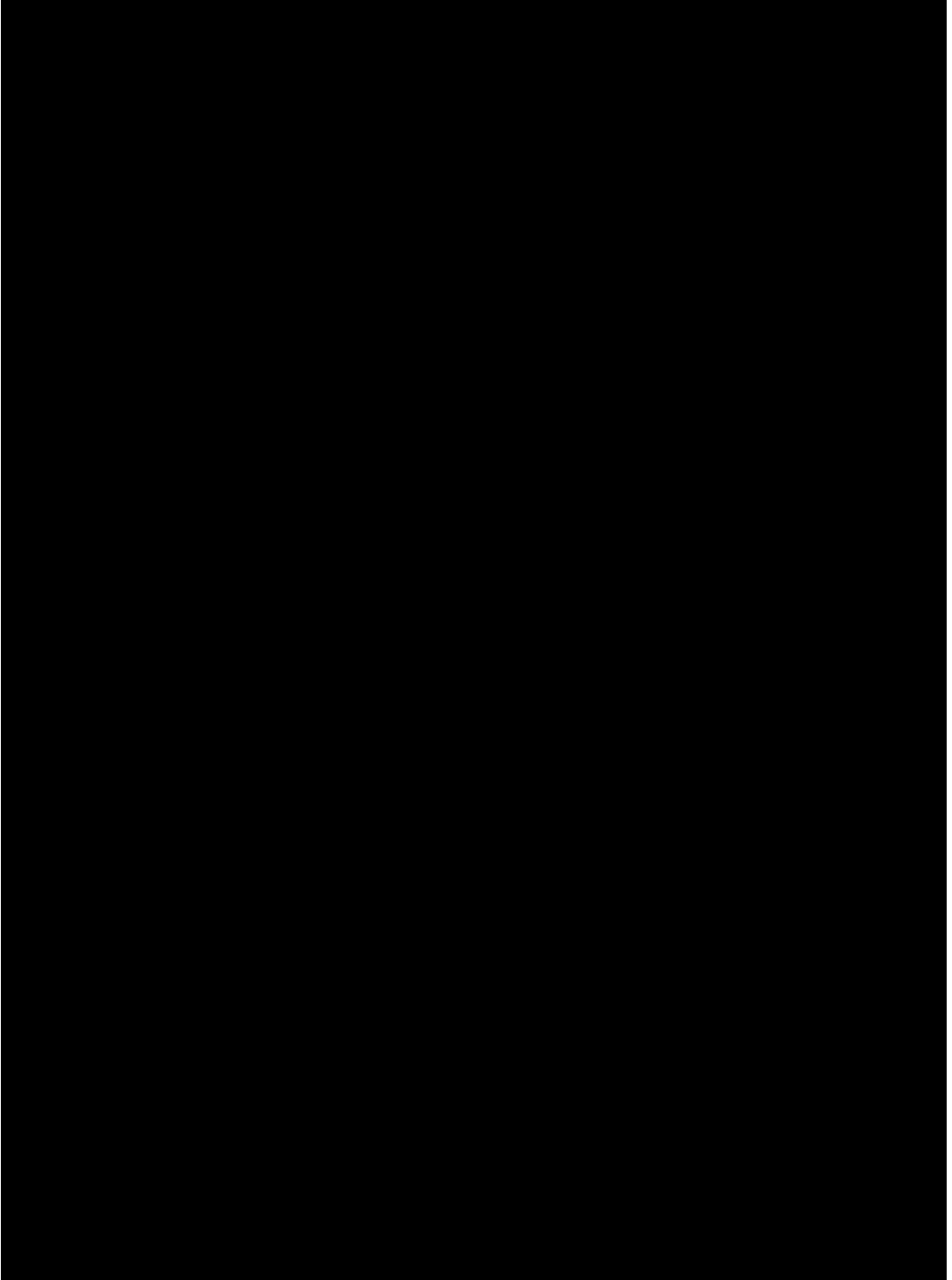
The Vendor shall provide three (3) references of customers utilizing the proposed solution fully implemented in a setting similar to this solicitation's scope of work. References within like North Carolina communities / industries are encouraged.

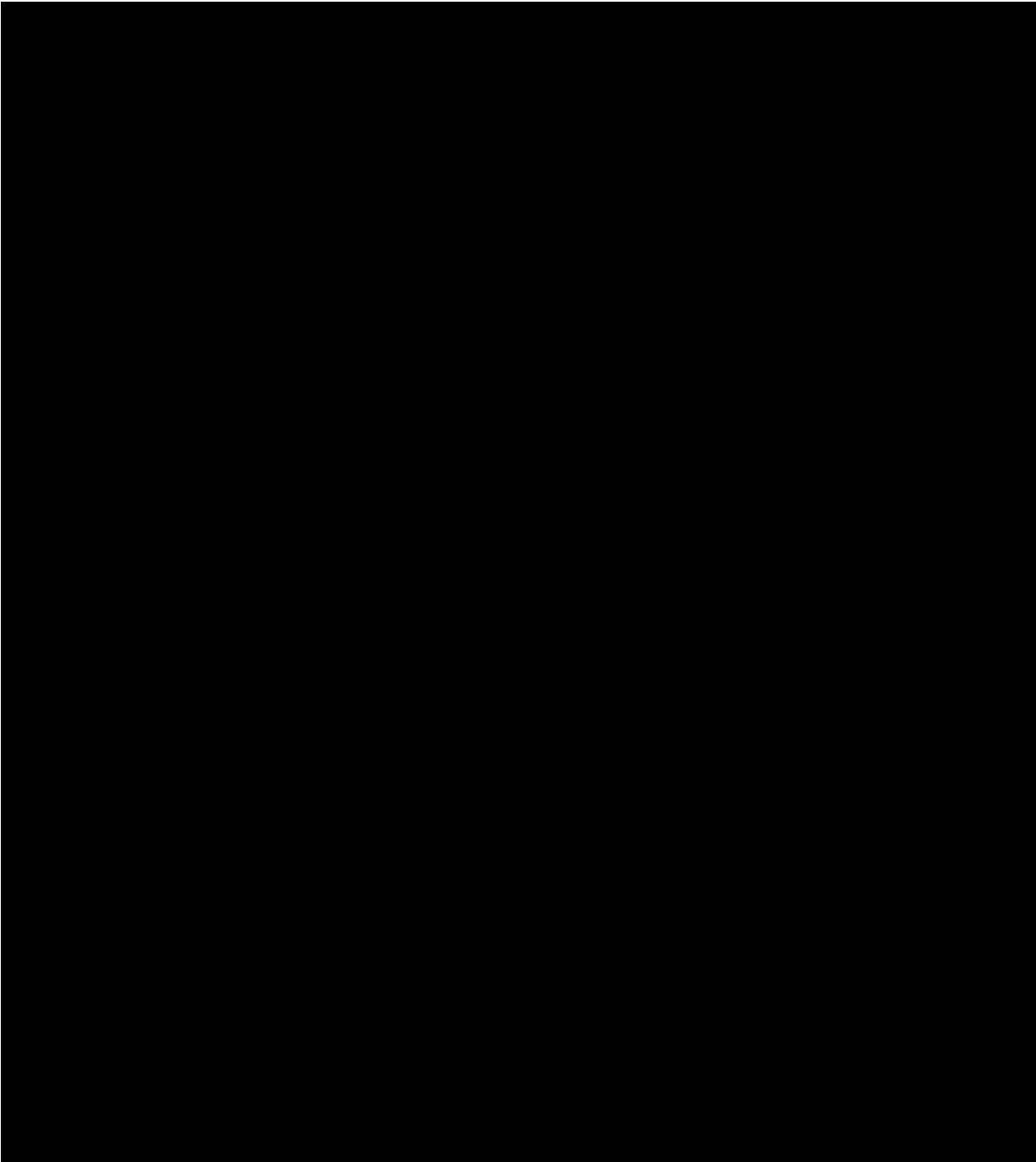
The Vendor should have implemented the respective proposed service within the last three (3) years. Customer references whose business processes and data needs are similar to those performed by the Agency needing this solution in terms of functionality, complexity, and transaction volume are encouraged.

For each reference, the Vendor shall provide the following information:

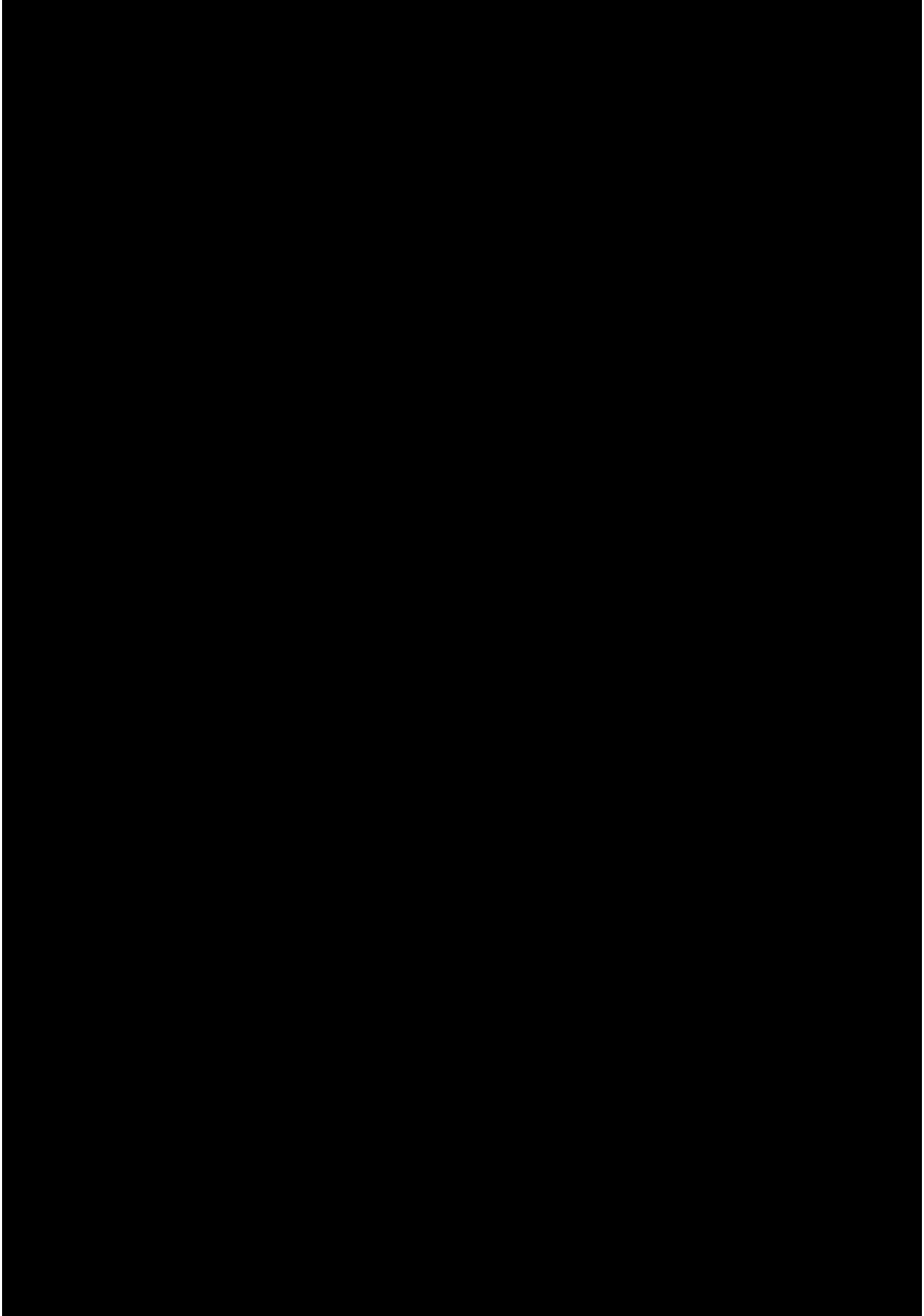
- a. Customer name.
- b. Customer address.
- c. Current telephone number of a customer employee most familiar with the offered solution implementation.
- d. Customer email address
- e. Time period over which each offered solution implementation was completed.
- f. Brief summary of the offered solution implementation.
- g. List of offered solution products installed and operational.
- h. Number of vendor or technical staff supporting, maintaining and managing the offered solution
- i. Number of end users supported by the offered solution.
- j. Number of sites supported by the offered solution.

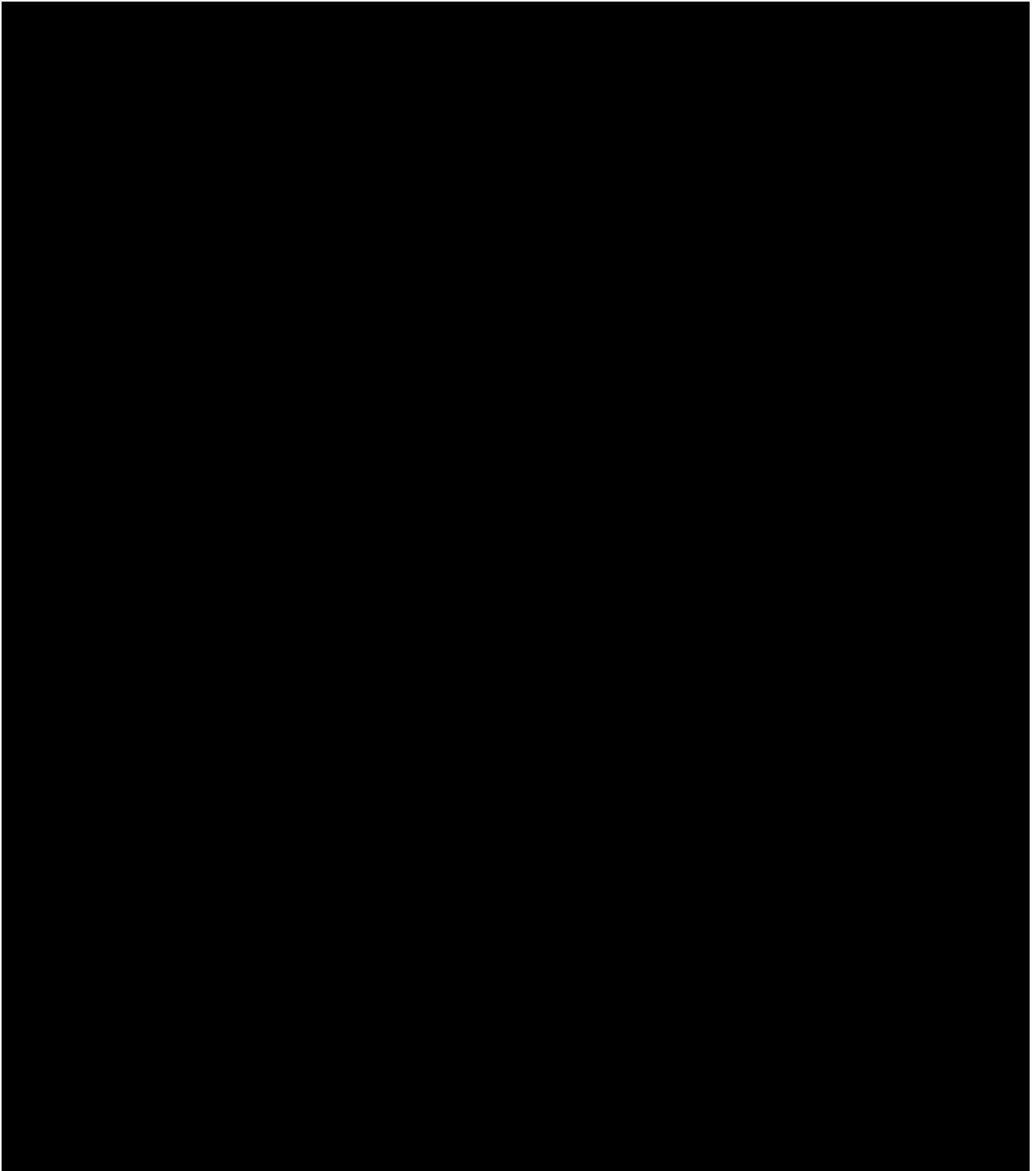
The information obtained will be considered in the evaluation of the proposal.



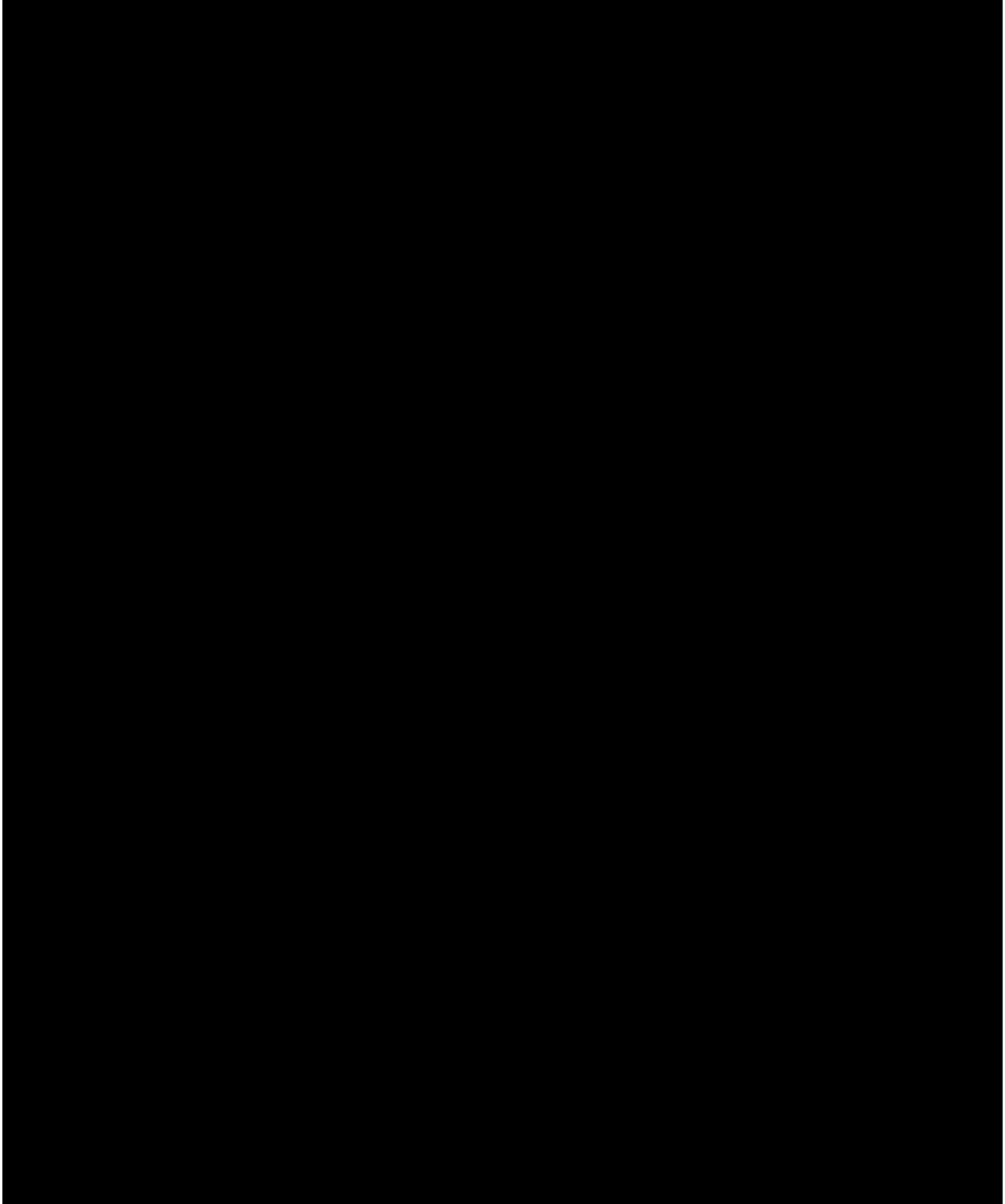


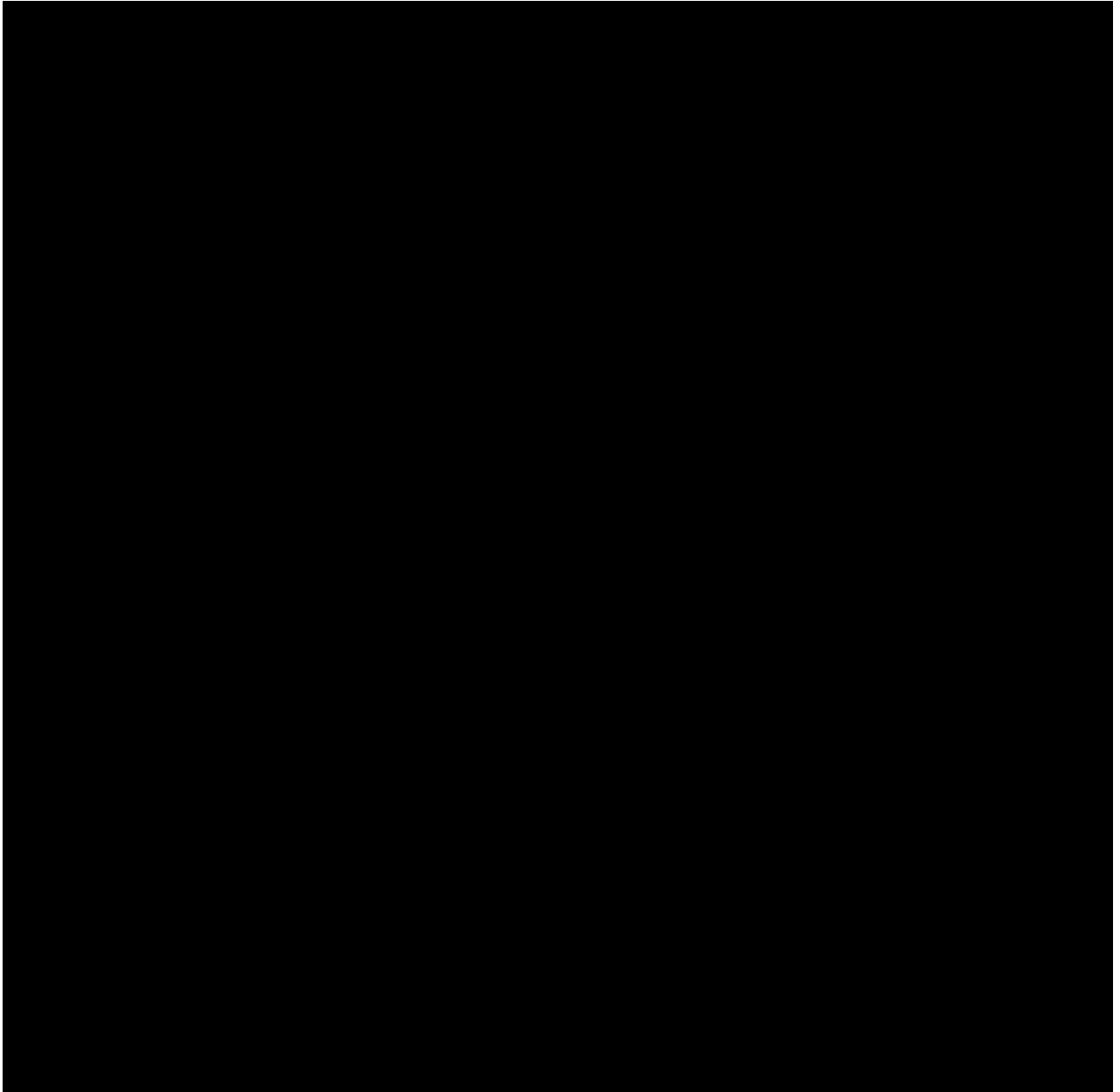
Reference 2 - USDA Animal and Plant Health Inspection Service (APHIS)





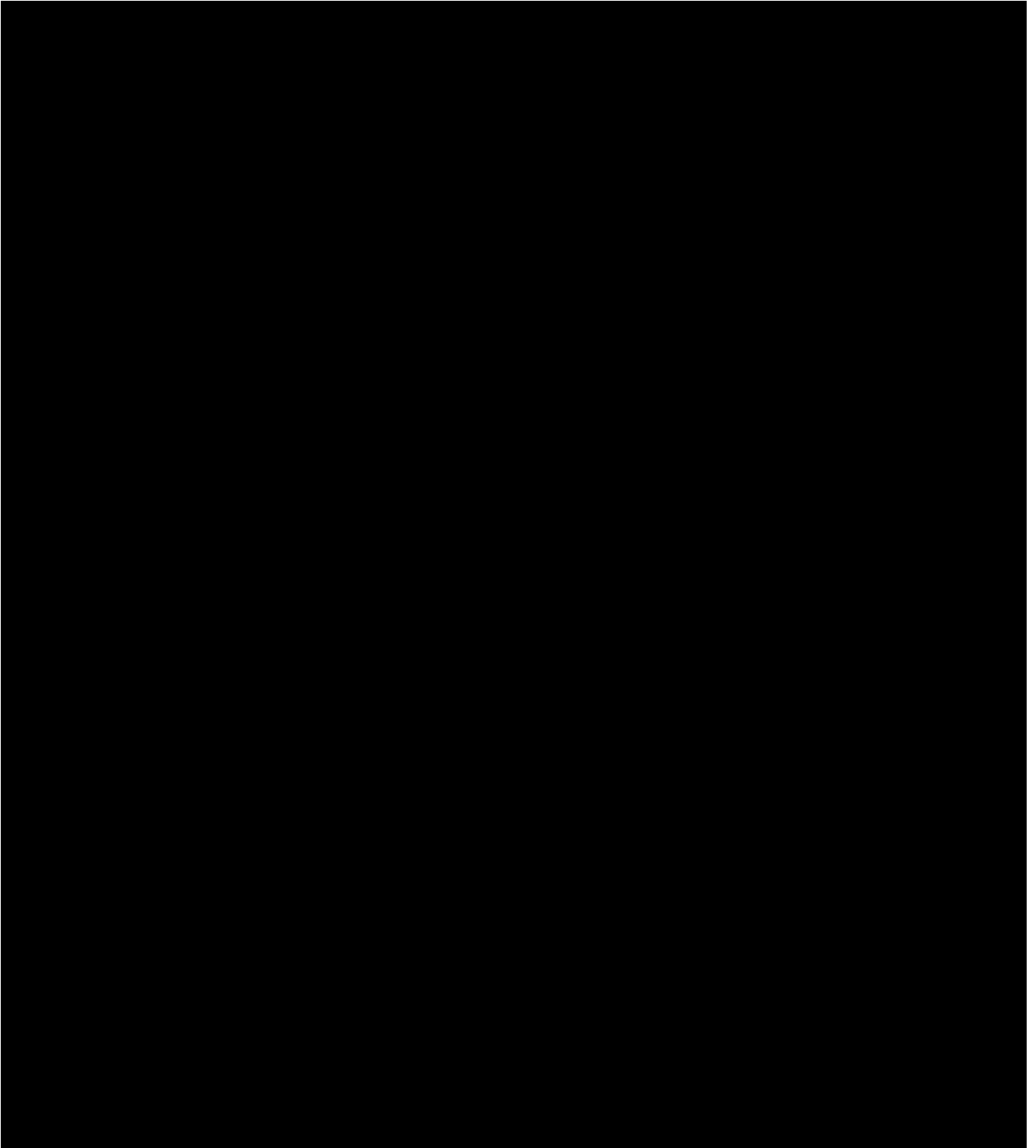
Reference 3 - State of North Carolina - Division of Child Development and Early Education





Reference 4 - Michigan Department of Health and Human Services










Section L)

Financial Statements (Attachment I)

L) Financial Statements (Attachment I)

Vendor shall review the Financial Review Form, provide responses in the gray-shaded boxes, and submit the completed Form as an Excel file with its offer. Vendor shall not add or delete rows or columns in the Form or change the order of the rows or column in the file.

ATTACHMENT I: FINANCIAL REVIEW FORM

1. Vendor Name	Accenture LLP		
2. Company Structure for tax purposes (C Corp, S Corp, LLC, LLP, etc.):	Limited Liability Partnership		
3. Have you been in business for more than three years?	Yes		
4. Has you filed for bankruptcy in the past three years?	No		
5. In the past three years, has your auditor issues any notification letters addressing significant issues? If yes, please explain and provide a copy of the notification letters.	No		
6. Are the financial figures below based on audited financial statements?	Yes		
7. Start Date of the financial statements:	9/1/2019		
End Date of the financial statements:	8/31/2022		
8. Provide a link to annual reports with financial statements and management discussion for the past three complete fiscal years.	 Accenture-Fiscal-2020-Annual-Report.pdf	 Accenture-Fiscal-2021-Annual-Report.pdf	 Accenture-Fiscal-2022-Annual-Report.pdf
9. Provide the following information for the past three complete fiscal years:	Last complete fiscal year minus two years	Latest complete fiscal year minus one year	Latest complete fiscal year
	9/1/2019 - 8/31/2020	9/1/2020 - 8/31/2021	9/1/2021 - 8/31/2022
BALANCE SHEET DATA			
Cash and Temporary Investments	\$ 8,415,330,000	\$ 8,168,174,000	\$ 7,889,833,000
Accounts Receivable (beginning of year)	\$ 8,095,071,000	\$ 7,846,892,000	\$ 9,728,212,000
Accounts Receivable (end of year)	\$ 7,846,892,000	\$ 9,728,212,000	\$ 11,776,775,000
Average Account Receivable for the Year (calculated)	\$ 7,970,981,500	\$ 8,787,552,000	\$ 10,752,494,000
Inventory (beginning of year)	\$ 0	\$ 0	\$ 0
Inventory (end of year)	\$ 0	\$ 0	\$ 0

Average Inventory for the Year (calculated)	\$ 0	\$ 0	\$ 0
Current Assets	\$ 17,749,756,000	\$ 19,666,511,000	\$ 21,610,871,000
Current Liabilities	\$ 12,662,590,000	\$ 15,708,867,000	\$ 17,523,496,000
Total Liabilities	\$ 19,579,420,000	\$ 23,078,729,000	\$ 24,516,302,000
Total Stockholders' Equity (beginning of year)	\$ 14,827,691,000	\$ 17,499,173,000	\$ 20,097,114,000
Total Stockholders' Equity (end of year)	\$ 7,499,173,000	\$ 20,097,114,000	\$ 22,747,088,000
Average Stockholders' Equity during the year (calculated)	\$ 16,163,432,000	\$ 18,798,143,500	\$ 21,422,101,000
INCOME STATEMENT DATA			
Net Sales	\$ 44,327,039,000	\$ 50,533,389,000	\$ 61,594,305,000
Cost of Goods Sold (COGS)	\$ 30,350,881,000	\$ 34,169,261,000	\$ 41,892,766,000
Gross Profit (Net Sales minus COGS) (calculated)	\$ 13,976,158,000	\$ 16,364,128,000	\$ 19,701,539,000
Interest Expense for the Year	\$ 33,071,000	\$ 59,492,000	\$ 47,320,000
Net Income after Tax	\$ 5,185,313,000	\$ 5,990,545,000	\$ 6,988,960,000
Earnings for the Year before Interest & Income Tax Expense	\$ 6,807,402,000	\$ 7,820,608,000	\$ 9,339,781,000
STATEMENT OF CASH FLOWS			
Cash Flow provided by Operating Activities	\$ 8,215,152,000	\$ 8,975,148,000	\$ 9,541,129,000
Capital Expenditures (property, plant, equipment)	\$ 599,132,000	\$ 580,132,000	\$ 717,998,000



Section m)

Errata and Exceptions, if any

m) Errata and Exceptions, if any

Any errata or exceptions to the State's requirements and specifications may be presented on a separate page labeled "Exceptions to Requirements and Specifications". Include references to the corresponding requirements and specifications of the Solicitation. Any deviations shall be explained in detail. The Vendor shall not construe this paragraph as inviting deviation or implying that any deviation will be acceptable. Offers of alternative or non-equivalent goods or services may be rejected if not found substantially conforming; and if offered, must be supported by independent documentary verification that the offer substantially conforms to the specified goods or services specification. If a vendor materially deviates from RFP requirements or specifications, its offer may be determined to be non-responsive by the State. Offers conditioned upon acceptance of Vendor Errata or Exceptions may be determined to be non-responsive by the State.

RFP REFERENCE	BRIEF EXPLANATION OF EXCEPTION
RFP, Attachment B: Department of Information Technology Terms and Conditions, Section 2: Terms and Conditions Applicable to Software as a Service (SaaS)	Accenture proposes to remove Section 2: Terms and Conditions Applicable to Software as a Service (SaaS) of Attachment B: Department of Information Technology Terms and Conditions in its entirety from the final agreement. Accenture's proposed solution separates SaaS components from the overall solution as a value add for NC DHHS to contract directly with our solution partners.
RFP, Attachment C: Department of Health and Human Services Terms and Conditions, Section C.3: Stabilization	Accenture proposes to reserve this section for discussion. The final language will be dependent on final agreement for SLA's. Accenture has proposed SLA's and performance measurements that would be effective after go live in Section R - Draft Service Level Agreement of this proposal

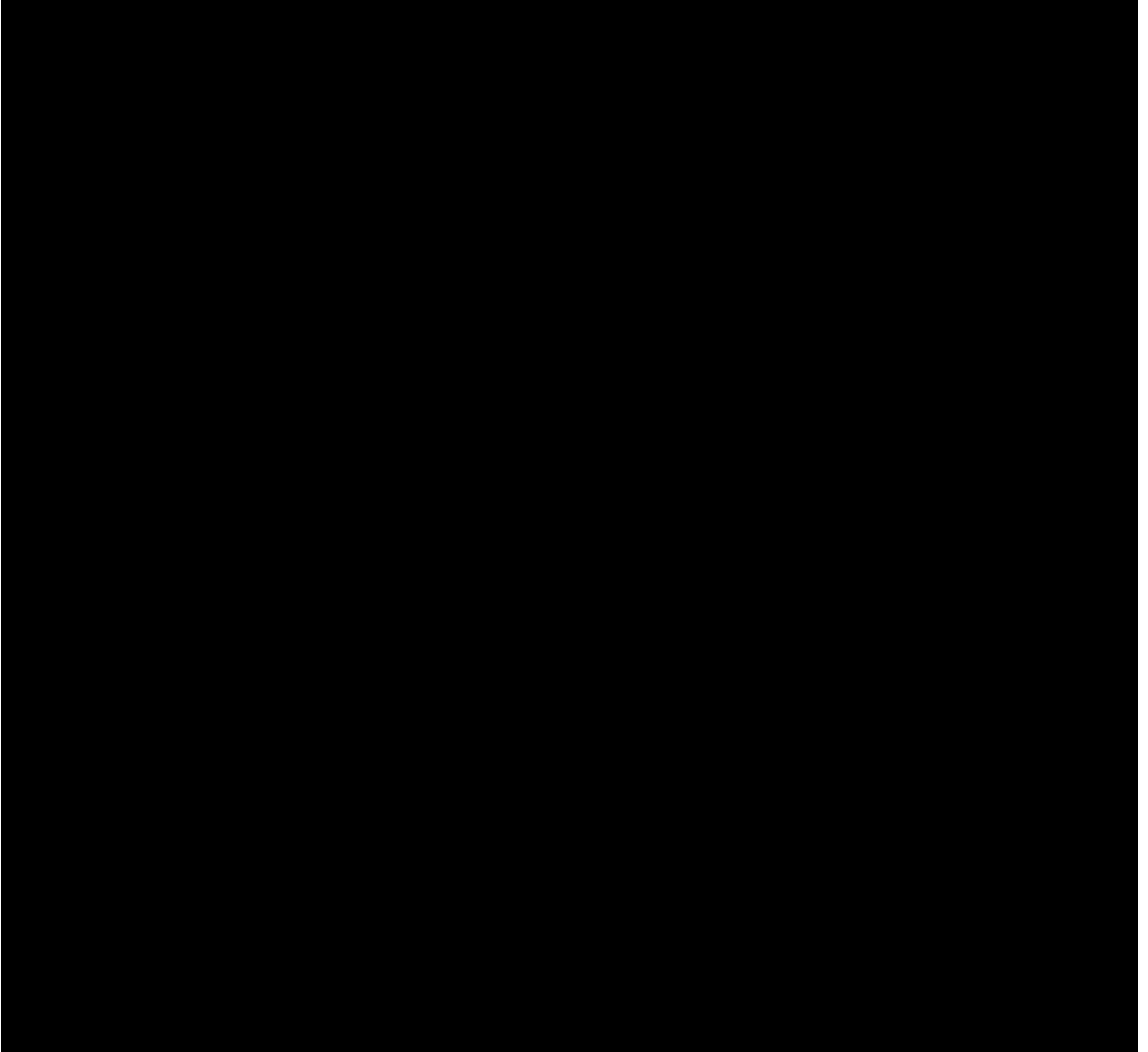
Accenture has reviewed RFP Attachment B: Department of Information Technology Terms and Conditions and has no other exceptions. Accenture is familiar with these terms from our other work in North Carolina and believes them to provide a fair and appropriate framework for these critical services.



Section n)

Vendor's License and Maintenance Agreements, if any, and Third-Party License Agreements, if any

n) Vendor's License and Maintenance Agreements, if any, and Third-Party License Agreements, if any





Section o)

Supporting material such as technical system documentation, training examples, etc.

o) Supporting material such as technical system documentation, training examples, etc.

No other supporting materials or documentation have been included with this response.

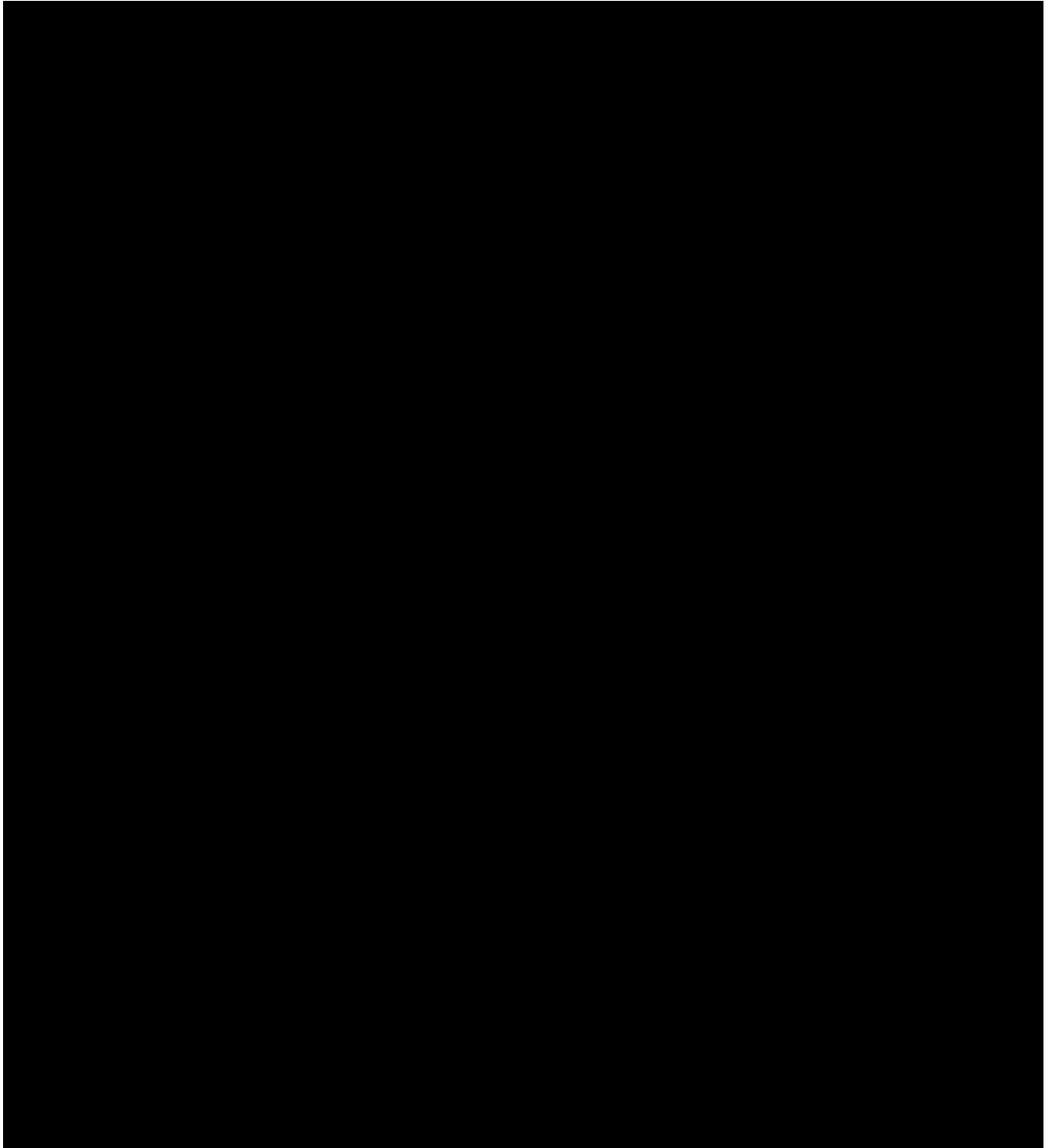


Section p)

Other supporting materials

p) Other supporting materials.

Vendor may attach other supporting materials that it feels may improve the quality of its response. These materials should be included as items in a separate appendix.





Section q)

All Pages of the Solicitation

q) All Pages of the Solicitation
(including Attachments A, B,
and C)

STATE OF NORTH CAROLINA Department of Health and Human Services	REQUEST FOR PROPOSAL NO. 30-23189	
	Offers will be publicly opened:	
	Issue Date: June 27, 2023	
Refer <u>ALL</u> inquiries regarding this RFP to: Maureen Salman Contract Specialist Office of Procurements, Contracts and Grants maureen.salman@dhhs.nc.gov	Commodity Number: 811118	
	Description: DCDEE - Workforce Registry and NC Pre-K and Regulatory System Replacement	
	Purchasing Agency: Department of Health and Human Services (DHHS), Division of Child Development and Early Education (DCDEE)	
	Requisition No.: 	

OFFER

The Purchasing Agency solicits offers for Services and/or goods described in this solicitation. All offers and responses received shall be treated as Offers to contract as defined in 9 NCAC 06A.0102(12).

EXECUTION

In compliance with this Request for Proposal, and subject to all the conditions herein, the undersigned offers and agrees to furnish any or all Services or goods upon which prices are offered, at the price(s) offered herein, within the time specified herein.

Failure to execute/sign offer prior to submittal shall render offer invalid. Late offers are not acceptable.

OFFEROR: Accenture LLP		
STREET ADDRESS:	P.O. BOX:	ZIP:
CITY, STATE & ZIP:	TELEPHONE NUMBER:	TOLL FREE TEL. NO
PRINT NAME & TITLE OF PERSON SIGNING:	FAX NUMBER:	
AUTHORIZED SIGNATURE:	DATE:	E-MAIL:

Offer valid for ninety (90) days from date of offer opening unless otherwise stated here: ____days

ACCEPTANCE OF OFFER

If any or all parts of this offer are accepted, an authorized representative of DCDEE shall affix its signature hereto and any subsequent Request for Best and Final Offer, if issued. Acceptance shall create a contract having an order of precedence as follows: Best and Final Offers, if any, Special terms and conditions specific to this RFP, Specifications of the RFP, the Department of Information Technology Terms and Conditions, Department of Health and Human Services Terms and Conditions, and the agreed portion of the awarded Vendor's Offer. A copy of this acceptance will be forwarded to the awarded Vendor(s).

FOR PURCHASING AGENCY USE ONLY	
Offer accepted and contract awarded this date	, as indicated on attached certification,
by	(Authorized representative of Purchasing Agency Name Error!
Reference source not found.)	

Table of Contents

1.0	ANTICIPATED PROCUREMENT SCHEDULE	4
2.0	PURPOSE OF RFP	5
2.1	INTRODUCTION	5
2.2	CONTRACT TERM	5
2.3	CONTRACT TYPE	5
2.4	AGENCY BACKGROUND	5
2.4.1.	<i>Department of Health and Human Services Mission</i>	<i>5</i>
2.4.2.	<i>Division of Child Development and Early Education Mission</i>	<i>6</i>
2.4.3.	<i>Responsibilities of DCDEE</i>	<i>6</i>
2.5	PROBLEM STATEMENT	6
2.6	CONTRACT PHASES	7
3.0	RFP REQUIREMENTS AND SPECIFICATIONS	8
3.1	GENERAL REQUIREMENTS AND SPECIFICATIONS	8
3.2	SECURITY REQUIREMENTS AND SPECIFICATIONS	9
3.3	ENTERPRISE SPECIFICATIONS	10
3.4	BUSINESS AND TECHNICAL SPECIFICATIONS	11
3.5	MANAGEMENT SPECIFICATIONS	11
3.5.1	<i>Software Development Lifecycle (SDLC)</i>	<i>11</i>
3.5.2	<i>Project Management</i>	<i>11</i>
3.5.3	<i>Testing</i>	<i>19</i>
3.5.4	<i>Training</i>	<i>20</i>
3.5.5	<i>Data Conversion and Migration</i>	<i>20</i>
3.5.6	<i>Operations and Maintenance</i>	<i>21</i>
4.0	COST OF VENDOR'S OFFER	26
4.1	OFFER COSTS	26
4.2	PAYMENT SCHEDULE	26
5.0	EVALUATION	26
5.1	SOURCE SELECTION	26
5.2	EVALUATION CRITERIA	27
5.3	BEST AND FINAL OFFERS (BAFO)	27
5.4	POSSESSION AND REVIEW	28
6.0	VENDOR INFORMATION AND INSTRUCTIONS	28
6.1	GENERAL CONDITIONS OF OFFER	28
6.2	GENERAL INSTRUCTIONS FOR VENDOR	29
6.3	INSTRUCTIONS FOR OFFER SUBMISSION	32
7.0	OTHER REQUIREMENTS AND SPECIAL TERMS	34
7.1	VENDOR UTILIZATION OF WORKERS OUTSIDE OF U.S.	34
7.2	FINANCIAL STATEMENTS	34
7.3	FINANCIAL RESOURCES ASSESSMENT, QUALITY ASSURANCE, PERFORMANCE AND RELIABILITY	35
7.4	VENDOR'S LICENSE OR SUPPORT AGREEMENTS	35
7.5	RESELLERS (RESERVE)	35
7.6	DISCLOSURE OF LITIGATION	35
7.7	CRIMINAL CONVICTION	36
7.8	SECURITY AND BACKGROUND CHECKS	36
7.9	ASSURANCES	36
7.10	CONFIDENTIALITY OF OFFERS	37
7.11	PROJECT MANAGEMENT	37
7.12	MEETINGS	37
7.13	RECYCLING AND SOURCE REDUCTION	38

7.14 INVOICES.....	39
7.15 SPECIAL TERMS AND CONDITIONS (RESERVED)	39
ATTACHMENT A: DEFINITIONS	40
ATTACHMENT B: DEPARTMENT OF INFORMATION TECHNOLOGY TERMS AND CONDITIONS	48
ATTACHMENT C: DEPARTMENT OF HEALTH AND HUMAN SERVICES TERMS AND CONDITIONS.....	71
ATTACHMENT D: DESCRIPTION OF OFFEROR	79
ATTACHMENT E: COST FORM	81
ATTACHMENT F: VENDOR CERTIFICATION FORM	87
ATTACHMENT G: LOCATION OF WORKERS UTILIZED BY VENDOR.....	88
ATTACHMENT H: REFERENCES	89
ATTACHMENT I: FINANCIAL REVIEW FORM	90
ATTACHMENT J: MINIMUM CONTENT FOR PROJECT AND O&M DELIVERABLES	92
ATTACHMENT K: REGULATORY MODERNIZATION BUSINESS SPECIFICATIONS.....	138
ATTACHMENT L: WORKFORCE REGISTRY BUSINESS SPECIFICATIONS.....	142
ATTACHMENT M: NC PRE-K SPECIFICATIONS.....	151
ATTACHMENT N: SUBSIDY PROVIDER COMPLIANCE BUSINESS SPECIFICATIONS.....	158
ATTACHMENT O: BUSINESS AND TECHNICAL SPECIFICATIONS	163
ATTACHMENT P: LIST OF REPORTS	170
ATTACHMENTS Q – MMM: WORKFLOW DIAGRAMS.....	171

1.0 ANTICIPATED PROCUREMENT SCHEDULE

The Agency Procurement Agent will make every effort to adhere to the following schedule:

Action	Responsibility	Date
RFP Issued	Agency	June 27, 2023
Written Questions Deadline	Potential Vendors	July 10, 2023
Agency's Response to Written Questions/ RFP Addendum Issued	Agency	July 21, 2023
Offer Opening Deadline	Vendor(s)	August 14, 2023, at 2:00 PM EST
Offer Evaluation	Agency	August 28, 2023
Selection of Finalists	Agency	September 19, 2023
Oral Presentations and/or Product Demonstrations by Finalists	Selected Vendors	September 1, 2023, through September 19, 2023
Negotiations with Finalists	Agency designees and selected Vendor(s)	September 20, 2023, through September 29, 2023
Best and Final Offers Deadline from Finalists	Selected Vendors	October 13, 2023
Contract Award	Agency	October 31, 2023
Protest Deadline	Responding Vendors	15 days after award

2.0 PURPOSE OF RFP

2.1 INTRODUCTION

The purpose of this RFP is to solicit offers for the purchase of a comprehensive, highly configurable and fully integrated Workforce Registry and PreK and Regulatory System solution ("Solution"), including Vendor provided technical, operational and maintenance support. The Solution may be hosted on State Infrastructure, hosted on Vendor provided infrastructure or a combination of the two. Either COTs software, Software as a Service (SaaS), or a combination thereof, is an acceptable solution for this RFP. (Vendors will need to include in their proposal if any COTs components are to be utilized in a SaaS solution.) The proposed Workforce Registry and PreK and Regulatory solution is needed to automate business processes and to improve the operational efficiency and effectiveness of the Early Education, Regulatory, and Subsidy Section staff of DCDEE. The system will serve as a secure, trusted source for information regarding licensed childcare facilities and early childcare professionals in NC.

2.2 CONTRACT TERM

A contract awarded pursuant to this RFP shall have an effective date as provided in the Notice of Award. The term shall be two (2) year(s) and will expire upon the anniversary date of the effective date unless otherwise stated in the Notice of Award, or unless terminated earlier. The State retains the option to extend the Agreement for one (1) one(1) year renewal period at its sole discretion.

2.2.1 EFFECTIVE DATE

This solicitation, including any Exhibits, or any resulting contract or amendment shall not become effective nor bind the State until the appropriate State purchasing authority/official, or Agency official has signed the document(s), contract or amendment; the effective award date has been completed on the document(s), by the State purchasing official, and that date has arrived or passed. The State shall not be responsible for reimbursing the Vendor for goods provided nor Services rendered prior to the appropriate signatures and the arrival of the effective date of the Agreement. No contract shall be binding on the State until an encumbrance of funds has been made for payment of the sums due under the Agreement.

2.3 CONTRACT TYPE

Definite Quantity Contract - This request is for a closed-ended contract between the awarded Vendor and the State to furnish a pre-determined quantity of a good or service during a specified period of time.

The State reserves the right to make partial, progressive, or multiple awards: where it is advantageous to award separately by items; or where more than one supplier is needed to provide the contemplated specifications as to quantity, quality, delivery, service, geographical areas; and where other factors are deemed to be necessary or proper to the purchase in question.

2.4 AGENCY BACKGROUND

2.4.1. Department of Health and Human Services Mission

The mission of the NC Department of Health and Human Services (DHHS) is, in collaboration with our partners, to provide essential human services to improve the health, safety and well-being of all North Carolinians.

The NC Division of Child Development and Early Education (DCDEE) is a division of the NC DHHS.

2.4.2. Division of Child Development and Early Education Mission

The mission of the Division of Child Development and Early Education (DCDEE) is to ensure the health and safety of children in childcare programs, to promote quality childcare by implementing evidenced-based standards and to increase access to quality childcare to families and children across North Carolina.

2.4.3. Responsibilities of DCDEE

1. To ensure the health and safety of children in childcare programs DCDEE:
 - Licenses, monitors and provides technical assistance to childcare programs.
 - Investigates any concerns regarding illegally operating childcare programs, as well as complaints alleging violations of childcare requirements.
 - Conducts comprehensive Criminal Background Checks with all individuals who work in licensed or regulated child care programs and other social and human services programs
 - Supports the NC Child Care Commission, which has responsibility to create, amend or repeal rules to implement Child Care Law.
2. Promotes quality childcare by implementing evidenced-based standards DCDEE:
 - Evaluates teacher and administrator education to determine qualification for different positions in childcare programs.
 - Licenses early childhood educators in non-public programs
 - Administers the NC Prekindergarten (NC Pre-K) program
 - Funds the statewide Child Care Resource and Referral system which provides evidence-based technical assistance, professional development, coaching and compensation supports for early childhood professionals
 - Works with a variety of early childhood partners to provide training, coaching, and evaluation for early childhood professionals across the state.
 - Collaborates with the state funded NC Partnership for Children/Smart Start
3. Increases access to quality childcare to families and children across North Carolina DCDEE:
 - Administers North Carolina's Subsidized Child Care Assistance program
 - Provides parents a web-based tool to search for quality childcare programs.
 - Collaborates with early childhood partners and homeless service providers to address the need for child care for families experiencing homelessness or temporary housing arrangements.
 - Administers NC's Child Care and Development Fund federal block grant.

2.5 PROBLEM STATEMENT

DCDEE has and uses multiple systems, through partners – DCDEE WORKS, Regulatory System, Scribbles, DPI Systems (Human Resources Management System (HRMS), NCDPI Online Licensure System (OLS)), CCSA Systems (which includes AWARDS, TEACH, WAGE\$) etc. – to support Early Education Branch

workforce and Regulatory Services Section needs. These systems do not interface with one another or provide real-time data.

The current process flow for Early Education Branch and Regulatory Services Section staff are highly manual, paper driven, and partially automated resulting in time-consuming processes and challenges in data reporting. Data inaccuracy and duplication is unavoidable when disparate systems are used bogging the team in administrative tasks. It also creates a burden on end-users to repeatedly provide the same or similar information to multiple systems. Overall, these challenges limit the ability to connect with the end-users.

Subsidy staff are accessing disparate data sources as well as sharing significant volumes of multiple forms, documents, and sizeable spreadsheets to manage information required to perform their work. Currently, the Staff uses a kluge of office tools and server stores to support their business processes which have become complex and multi-tiered. Because data management tasks are largely manual, the data management tasks have extremely tedious and inefficient, and introduces unacceptable risks to data security and fidelity. In addition, all managed information is subject to audit and may be used as evidence in judicial proceedings, which means that data security, fidelity, and ready accessibility are critical components of subsidy staff's ability to effectively conduct their business.

The NC Pre-K program, currently, uses 3 separate applications to complete their day- to-day work. These applications are outdated and do not meet current technology standards. The NC Pre-K program is used throughout the state of NC and needs to be modernized.

See the workflow models in *Attachments Q through TT* illustrating the business processes representative of where the problems referred to exist for added context. Additionally, the Attachments reflect current and future state context diagrams that model internal and external entities with which the indicated business does/will interface respectively. See attachment P for a sample of reports currently generated.

DCDEE must have a fully implemented new solution complete and in use by the end of September, 2024.

2.6 CONTRACT PHASES

This RFP will address two (2) distinct Contract Phase: The Project Execution Contract Phase to implement the Solution and the Operations and Maintenance (O&M) Contract Phase to maintain the Solution, as outlined below:

- 2.6.1.** The Project Execution Contract Phase sections in this document will explain the approach, Deliverables and tasks/activities that will occur to configure the Vendor's product to implement the Solution. During these activities, the Vendor will execute all Solution implementation tasks (i.e., requirements definition, development/configuration, testing, pilot, and training) until the Solution is deployed. For additional information about the Project, refer to Section III. 12) c) ii. 2.; Section V. 9) and 10); and *Attachment J. Minimum Content Requirements for Project and O&M Deliverables*.

The Solution must be fully deployed no later than September 30, 2024.

- 2.6.2.** The O&M Contract Phase sections in this document will explain the approach, Deliverables and tasks/activities that will occur in this phase. During this phase, the Vendor will complete all Deliverables and execute all tasks/activities related to operating and maintaining the Solution. In addition, the Vendor will maintain the hosting environment (if Vendor-hosted Solution is selected) or provide support and updates/new releases for the product the Solution is based on (if State-hosted Solution is selected), as well as modify the Solution if requested by the Agency. For

additional information about Operations and Maintenance, refer to Section 3.5.6 and *Attachment J, Minimum Content for Project and O&M Deliverables*.

3.0 RFP REQUIREMENTS AND SPECIFICATIONS

3.1 GENERAL REQUIREMENTS AND SPECIFICATIONS

3.1.1 REQUIREMENTS

Means, as used herein, a function, feature, or performance that the system must provide. See subsequent sections for requirements.

3.1.2 SPECIFICATIONS

Means, as used herein, a specification that documents the function and performance of a system or system component.

The apparent silence of the specifications as to any detail, or the apparent omission of detailed description concerning any point, shall be regarded as meaning that only the best commercial practice is to prevail and that only processes, configurations, materials and workmanship of the first quality may be used. Upon any notice of noncompliance provided by the State, Vendor shall supply proof of compliance with the specifications. Vendor must provide written notice of its intent to deliver alternate or substitute Services, products, goods or other Deliverables. Alternate or substitute Services, products, goods or Deliverables may be accepted or rejected in the sole discretion of the State; and any such alternates or substitutes must be accompanied by Vendor's certification and evidence satisfactory to the State that the function, characteristics, performance and endurance will be equal or superior to the original Deliverables specified.

3.1.3 SITE AND SYSTEM PREPARATION

Vendors shall provide the Purchasing State Agency complete site requirement specifications for the Deliverables, if any. These specifications shall ensure that the Deliverables to be installed or implemented shall operate properly and efficiently within the site and system environment. Any alterations or modification in site preparation, which are directly attributable to incomplete or erroneous specifications provided by the Vendor and which would involve additional expenses to the State, shall be made at the expense of the Vendor.

3.1.4 EQUIVALENT ITEMS

Whenever a material, article or piece of equipment is identified in the specification(s) by reference to a manufacturers or Vendor's name, trade name, catalog number or similar identifier, it is intended to establish a standard for determining substantial conformity during evaluation, unless otherwise specifically stated as a brand specific requirement (no substitute items will be allowed). Any material, article or piece of equipment of other manufacturers or Vendors shall perform to the standard of the item named. Equivalent offers must be accompanied by sufficient descriptive literature and/or specifications to provide for detailed comparison.

3.1.5 ENTERPRISE LICENSING

In offering the best value to the State, Vendors are encouraged to leverage the State's existing resources and license agreements, which can be viewed here:

<https://it.nc.gov/resources/statewide-it-procurement/statewide-it-contracts>

- a) Identify components or products that are needed for your solution that may not be available with the State's existing license agreement.
- b) Identify and explain any components that are missing from the State's existing license agreement.
- c) If the Vendor can provide a more cost-effective licensing agreement, please explain in detail the agreement and how it would benefit the State.

3.2 SECURITY REQUIREMENTS AND SPECIFICATIONS

The State is seeking a solution that is either hosted on State Infrastructure or hosted on Vendor provided Infrastructure depending on the solution the Vendor recommends.

3.2.1 SOLUTIONS HOSTED ON STATE INFRASTRUCTURE

Vendors shall provide a completed Vendor Readiness Assessment Report State Hosted Solutions ("VRAR") at offer submission. This report is located at the following website:

<https://it.nc.gov/documents/vendor-readiness-assessment-report>

The Registry, NC Pre-K, and Regulatory Systems will be required to receive and securely manage data that is classified as medium and high risk. Refer to the North Carolina Statewide Data Classification and Handling policy for more information regarding this data classification. The policy is located at the following website: <https://it.nc.gov/document/statewide-data-classification-and-handling-policy>.

To comply with the State's Security Standards and Policies, State agencies are required to perform annual security/risk assessments on their information systems using NIST 800-53 controls.

3.2.2 SOLUTIONS NOT HOSTED ON STATE INFRASTRUCTURE

The Registry, NC Pre-K, and Regulatory systems will be required to receive and securely manage data that is classified as medium and high risk. Refer to the North Carolina Statewide Data Classification and Handling policy for more information regarding data classification. The policy is located at the following website: <https://it.nc.gov/document/statewide-data-classification-and-handling-policy>.

To comply with the State's Security Standards and Policies, State agencies are required to perform annual security/risk assessments on their information systems using NIST 800-53 controls. This requirement additionally applies to all Vendor-provided, agency-managed Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) solutions which will handle data classified as Medium Risk (Restricted) or High Risk (Highly Restricted) data.

- (a) Vendors shall provide a completed Vendor Readiness Assessment Report Non-State Hosted Solutions ("VRAR") at offer submission. This report is located at the following website: <https://it.nc.gov/documents/vendor-readiness-assessment-report>
- (b) Upon request, Vendors shall provide a current independent 3rd party assessment report in accordance with the following subparagraphs (i)-(iii) prior to contract award. However, Vendors are encouraged to provide a current independent 3rd party assessment report in accordance with subparagraphs (i)-(iii) at the time of offer submission.

(i) Federal Risk and Authorization Management Program (FedRAMP) certification, SOC 2 Type 2, ISO 27001, or HITRUST are the preferred assessment reports for any Vendor solutions which will handle data classified as Medium Risk (Restricted) or High Risk (Highly Restricted).

(ii) A Vendor that cannot provide a preferred independent 3rd party assessment report as described above may submit an alternative assessment, such as a SOC 2 Type 1 assessment report. The Vendor shall provide an explanation for submitting the alternative assessment report. If awarded this contract, a Vendor who submits an alternative assessment report shall submit one of the preferred assessment reports no later than 365 days of the Effective Date of the contract. Timely submission of this preferred assessment report shall be a material requirement of the contract.

(iii) An IaaS vendor cannot provide a certification or assessment report for a SaaS provider UNLESS permitted by the terms of a written agreement between the two vendors and the scope of the IaaS certification or assessment report clearly includes the SaaS solution.

(c) Additional Security Documentation. Prior to contract award, the State may in its discretion require the Vendor to provide additional security documentation, including but not limited to vulnerability assessment reports and penetration test reports. The awarded Vendor shall provide such additional security documentation upon request by the State during the term of the contract.

3.3 ENTERPRISE SPECIFICATIONS

3.3.1 ENTERPRISE STRATEGIES, SERVICES, AND STANDARDS

Agencies and vendors should refer to the Vendor Resources Page for information on North Carolina Information Technology enterprise services, security policies and practices, architectural requirements, and enterprise contracts. The Vendor Resources Page can be found at the following link: <https://it.nc.gov/vendor-engagement-resources>. This site provides vendors with statewide information and links referenced throughout the RFP document. Agencies may request additional information.

3.3.2 ARCHITECTURE DIAGRAMS DEFINED

The State utilizes architectural diagrams to better understand the design and technologies of a proposed solution. These diagrams (i.e., Network Diagram and Technology Stack Diagram), required at offer submission, can be found at the following link: <https://it.nc.gov/architectural-artifacts>.

There may be additional architectural diagrams requested of the vendor after contract award. This will be communicated to the vendor by the agency as needed during the project.

3.3.3 VIRTUALIZATION

The State desires the flexibility to host Vendor's proposed solution in a virtualized environment, should it determine in the future that virtualized hosting for such solution would be more economical or efficient. The State currently utilizes server virtualization technologies including VMware, Solaris and zLinux. The Vendor should state whether its solution operates in a virtualized environment. Vendor also should identify and describe all differences, restrictions or limitations of its proposed solution with respect to operation, licensing, support, certification, warranties, and any other details that may impact its proposed solution when hosted in a virtualized environment.

3.3.4 IDENTITY AND ACCESS MANAGEMENT (IAM)

The proposed solution must externalize identity and access management. The protocols describing the State's Identity and Access Management can be found at the following link:

<https://it.nc.gov/services/vendor-engagement-resources#identity-access-management>

Describe how your solution supports the above protocols as well as making them available for application integration/consumption.

3.4 BUSINESS AND TECHNICAL SPECIFICATIONS

REFER TO THE FOLLOWING ATTACHMENTS:

ATTACHMENT K, REGULATORY MODERNIZATION BUSINESS SPECIFICATIONS

ATTACHMENT L, WORKFORCE REGISTRY BUSINESS SPECIFICATIONS

ATTACHMENT M, NC PRE-K SPECIFICATIONS

ATTACHMENT N, SUBSIDY PROVIDER COMPLIANCE BUSINESS SPECIFICATIONS

SEE ATTACHMENT O. BUSINESS AND TECHNICAL SPECIFICATIONS

3.5 MANAGEMENT SPECIFICATIONS

The following specifications concern specific tasks to be completed during the Contract term, which will be divided into the Project Execution Contract Phase and Operations and Maintenance (O&M) Contract Phase. This section also requests additional information about the Vendor's proposed Project and ongoing O&M support approach, including partnership with State IT and Business personnel for delivery.

Awarded Vendor will complete delivery (defined as Agency acceptance of the stabilized solution) no later than September 30, 2024.

3.5.1 Software Development Lifecycle (SDLC)

Describe the SDLC approach, methodology, and tools you will use for supporting the Agency in delivering the proposed Solution, including Changes made to the Solution. The Agency requests use of agile-based methodologies.

3.5.2 Project Management

1. Vendor Project Management Approach

The State's framework employs decision points throughout the project for approval to proceed with next tasks (reference <https://it.nc.gov/programs/project-portfolio-management/quality-management-system>). The project stages in which the Vendor will be engaged include the Planning and Design Phase, Execution and Build, Implementation and Closeout phases. Reference Section 7.11 for additional information about Project Management.

Describe your approach to Project Management to be utilized in support of the State's project management framework, including:

- a. All project management tools needed to deliver the Solution and meet Business and Technical and Management Specifications.

- b. Approach and tasks for monitoring and controlling the project's schedule, scope, budget/resource tracking, risks, issues, change and quality.

The State prefers use of Agile frameworks.

2. Vendor Project and O&M Deliverables

Describe your approach to complete, or assist State personnel in completing, all Project Deliverables according to the Vendor Responsibilities listed in the table provided below in this section during the Project Execution Contract Phase and the O&M Contract Phase. If the Vendor Responsibility is listed as Contributor for a Project Management Deliverable, then the State is the Owner and is responsible for the completion of the Project Management Deliverable, with Vendor assistance. If the Vendor is listed as the Owner, then the Vendor is responsible for completion of the Project Management Deliverable, with State assistance (i.e., State is the Contributor).

Reference *Attachment J: Minimum Content for Project and O&M Deliverables* for description of and provision requirements for Project Management Deliverables. (The requirements set forth in *Attachment J: Minimum Content for Project and O&M Deliverables* apply to the deliverables during the contract term.)

<i>Project & O&M Deliverable</i>	<i>Vendor Responsibility for Project Execution Contract Phase</i>	<i>Vendor Responsibility for O&M Contract Phase</i>
Kick-Off Meeting	Contributor	n/a
Project Kick-Off Meeting Report	Owner	n/a
Executed Escrow Agreement and Escrowed Solution Source Code (if COTS product(s) are included in the proposal)	Owner	n/a
Vendor Project Schedule	Owner	n/a
Vendor Project Management Plan	Owner	n/a
Vendor Project Staffing Plan	Owner	n/a
Project Communication Plan and Communications Matrix	Contributor	n/a
Project Risk and Issues Management Plan, Project Risk Watch List Matrix, and Project Issues Log	Contributor	n/a

<i>Project & O&M Deliverable</i>	<i>Vendor Responsibility for Project Execution Contract Phase</i>	<i>Vendor Responsibility for O&M Contract Phase</i>
Vendor Software Quality Assurance Plan	Owner	Review and update every twelve (12) months or when impacted
Project Change Management Plan, Project Change Request Form, and Project Change Request Log	Contributor	n/a
Security Plan	Vendor-Hosted Solution: Owner ; or State-Hosted Solution: Contributor	Review and update every twelve (12) months or when impacted
Technical Architecture Diagrams	Owner	Owner
Configuration and Release Management Plan	Owner	Review and update every twelve (12) months or when impacted
Training Plan	Owner	Review and update every twelve (12) months or when impacted
Test Plan (Technical Testing; see also dedicated Data Migration and Performance Test Plans below)	Owner	Review and update every twelve (12) months or when impacted
Deployment Plan	Owner	Review and update every twelve (12) months or when impacted
Gap Analysis Document	Owner	n/a

<i>Project & O&M Deliverable</i>	<i>Vendor Responsibility for Project Execution Contract Phase</i>	<i>Vendor Responsibility for O&M Contract Phase</i>
System Requirements Document	Owner	Update when impacted
Solution/Sprint Backlogs	Solution Backlog: Contributor Sprint Backlog: Owner	Contributor
Use Cases	Owner	Owner
User Stories	Contributor	Contributor
Requirements Traceability Matrix	Owner	Owner
Data Model	Owner	Update when impacted
Data Dictionary	Owner	Update when impacted
Detailed Design Specifications Document	Owner	Review and update when impacted
Infrastructure Requirements (State-Hosting Option only)	Owner	Update when impacted
Infrastructure Configuration Specifications (State-Hosting Option only)	Owner	Update when impacted
Vendor Recommendation for Technical Training for State IT Support Personnel	Owner	Update when impacted
Configured State Technical Environments (for State-Hosting Option)	Contributor	n/a
Technical Skills Transfer (State-Hosting Option only)	Owner	Update when impacted

<i>Project & O&M Deliverable</i>	<i>Vendor Responsibility for Project Execution Contract Phase</i>	<i>Vendor Responsibility for O&M Contract Phase</i>
Base Product and Base Product Installation Instructions (for COTS products with State-Hosting Option)	Owner	Owner for new product releases
Assist the State to install the Base Product(s) (for COTS products with State-Hosting Option)	Owner	Owner for new product releases
Design Review Sessions	Owner	Owner
Test Cases	Owner	Owner
Test Scripts	Owner	Owner
Prepare and Demonstrate All Test Environments	Vendor-Hosted Environments: Owner State-Hosted Testing Environments: Contributor	Vendor-Hosted Environments: Maintain testing environments as needed State-Hosted Testing Environments: Contributor
Unit Test Results Report	Owner	Owner
System Test Results Report	Owner	Owner
Regression Test Results Report	Owner	Owner
Integration Test Results Report	Owner	Owner
Accessibility Test Results Report	Owner	Owner
Demonstration of Tested System	Owner	Owner
General Backup and Recovery Plan	Vendor-Hosted Solution: Owner State-Hosted Solution: Contributor	Review and update every twelve (12) months or when impacted

<i>Project & O&M Deliverable</i>	<i>Vendor Responsibility for Project Execution Contract Phase</i>	<i>Vendor Responsibility for O&M Contract Phase</i>
Disaster Recovery Plan	Vendor-Hosted Solution: Owner State-Hosted Solution: Contributor	Review and update every twelve (12) months or when impacted
Performance Test Plan	Vendor-Hosted Solution: Owner State-Hosted Solution: Contributor	Vendor-Hosted Solution: Owner State-Hosted Solution: Contributor
Performance Test Cases	Vendor-Hosted Solution: Owner State-Hosted Solution: Contributor	Vendor-Hosted Solution: Owner State-Hosted Solution: Contributor
Performance Test Scripts	Vendor-Hosted Solution: Owner State-Hosted Solution: Contributor	Vendor-Hosted Solution: Owner State-Hosted Solution: Contributor
Performance Test Readiness Report	Vendor-Hosted Solution: Owner State-Hosted Solution: Contributor	Vendor-Hosted Solution: Owner State-Hosted Solution: Contributor
Performance Test Results Report	Vendor-Hosted Solution: Owner State-Hosted Solution: Contributor	Vendor-Hosted Solution: Owner State-Hosted Solution: Contributor
Agency Approval of Performance	Owner	Owner
Data Conversion and Migration Plan	Owner	n/a
Data Map	Owner	n/a
Data Conversion Test Cases/Scripts	Owner	n/a

<i>Project & O&M Deliverable</i>	<i>Vendor Responsibility for Project Execution Contract Phase</i>	<i>Vendor Responsibility for O&M Contract Phase</i>
Data Conversion and Migration Test Results Report	Owner	n/a
Agency Acceptance of the Converted and Migrated Data	Owner	n/a
User Acceptance Test Plan	Contributor	Contributor
UAT Test Cases and Test Scripts	Contributor	Contributor
UAT Training Materials	Owner	Owner
UAT Training	Owner	Owner
UAT Results Report	Contributor	Contributor
Agency Acceptance of Tested Solution (for all releases or deployment phases)	Owner	Owner
User Guides, Quick Reference Guides, and Online Help Documentation	Owner	Owner
Technical and System Administration Documentation	Owner	Owner
Service Level Agreement(s)	Owner	Review and update every twelve (12) months or when impacted
Training Materials	Owner	Owner
Training Delivery	Owner	Owner
Operations and Maintenance Plan (State Hosting option only)	Owner	Review and update every twelve (12) months or when impacted

<i>Project & O&M Deliverable</i>	<i>Vendor Responsibility for Project Execution Contract Phase</i>	<i>Vendor Responsibility for O&M Contract Phase</i>
Release/Deployment Readiness Checklist	Contributor	Contributor
Completed Release/Deployment Readiness Checklist (For all releases or deployment phases)	Contributor	Contributor
Onsite Assistance during Release/Deployment Readiness (State-Hosted Solutions only)	Owner	Owner
Vendor Operations and Maintenance Staffing Plan	Owner	Update when impacted
Onsite Assistance during Release/Deployment (State-Hosted Solutions only)	Owner	Owner
Validation Test Results Report	Owner	Owner
Deployment UAT Results Report	Contributor	Contributor
Agency Acceptance of Deployment UAT Results (For all releases or all deployment phases)	Owner	Owner
Vendor Support during the Stabilization Period	Owner	n/a
Agency Acceptance of the Stabilized Solution	Owner	n/a
Lessons Learned	Contributor	n/a
Project Status Meetings	Contributor	n/a
Project Status Reports	Owner	n/a
Sprint Reports	Owner	Owner

<i>Project & O&M Deliverable</i>	<i>Vendor Responsibility for Project Execution Contract Phase</i>	<i>Vendor Responsibility for O&M Contract Phase</i>
Operations and Maintenance Status Reports	Owner	Owner
Transition Plan	Owner	Owner
Project Peer Review	Contributor	n/a

3. Vendor Project Staffing

Vendors are to include a draft project schedule in their response that includes and describes all planning activities, development activities, pilot, and deployment as well as the Project Management Deliverables listed in Section 3.5.2.2 above. For each Project and O&M Deliverable in the table above, Vendor shall identify Vendor and/or State personnel required to complete the task in the project schedule.

4. Releases/Production Deployment and Support

Describe your approach to deploying the developed Solution for production use, including the following items below in your RFP response:

- The strategy for deploying the Solution for production use, including the number of Releases proposed;
- Deployment planning and preparation, including site visits, site readiness verification, end user device upgrades;
- Security considerations;
- Hardware, software or facilities needed to support the deployment if the Solution proposed will not hosted by the Vendor;
- The deployment activities and reference to any milestones proposed by the Vendor;
- The roles and responsibilities to complete the deployment;
- Support provided during deployment, including onsite support; and
- Support provided during the Stabilization Period.

Refer to *Attachment J, Minimum Content for Project and O&M Deliverables* for the Agency's expectations regarding Solution deployment.

3.5.3 Testing

Describe your testing processes for the Solution in detail, specifically:

- a. Your approach to conducting all types of technical testing needed prior to User Acceptance Testing, each release/deployment, including pilot deployment, and post-deployment validation.
- b. Your proposed approach to UAT, data conversion testing, and performance testing.
- c. A description of the testing environment(s) and any specific software tools that you intend to use or make available for State use for all types of testing.
- d. How any test results for any Vendor-performed testing are presented for the Agency approval.
- e. Your proposed process for identifying, prioritizing, resolving, and documenting Defects found in the Solution during testing. Include in your description any software tools that you intend to make available for Defect management.
- f. How these tools will be integrated with DHHS tools including HP Quality Center/ALM, Jira, and Confluence.

Address all the test-related items described in Section 3.5.2.2 and *Attachment J, Minimum Content for Project and O&M Deliverables*.

3.5.4 Training

Describe your approach to training, identifying the points in your SDLC where training will occur for each type of training that you will provide to User Acceptance Testers, pilot users, end users, State Trainers, and State IT support staff. Include in this description:

- a. The training content that you will provide for the Solution, including the approach for in-person, remote, or pre-recorded training. Reference Section 3.5.2.2 and *Attachment J, Minimum Content for Project and O&M Deliverables* for details regarding the Agency's training documentation needs.
- b. Describe the training technical (hosting) environment for the Solution. Include in your description how your training technical environment addresses the following items:
 - i. Configurable mirror production functionality, and
 - ii. Online help.
- c. Describe how you provide training and knowledge transfer training to the Agency and other State IT staff as needed to assist Solution development efforts, system administration, and ongoing support for your proposed Solution.
- d. Describe any on demand training resources available to users such as recorded training sessions, computer-based training, FAQs, community forums, etc.
- e. Training provided during the O&M Contract Phase for new releases, enhancements, and any other changes to the Solution's underlying technology or hosting environment.

3.5.5 Data Conversion and Migration

Describe the Vendor's approach to converting and migrating data from existing systems (Regulatory (SQL), WORKS (Oracle), etc.) to the Solution. Include a list of all tools that will be used, and State resources required.

3.5.6 Operations and Maintenance

1. Vendor Approach to Operations and Maintenance

O&M will start after the Solution is deployed and the Vendor has obtained documentation of Agency Acceptance of the Stabilized Solution (i.e., the Stabilization Period has been successfully completed). The Vendor, when offering a Vendor-hosted Solution, will maintain the hardware and operating systems needed to host the Solution and updating the Solution with product patches and new releases.

Describe the Vendor's plan to perform/provide all O&M tasks/Deliverables. Reference 3.5.2.2 and *Attachment J, Minimum Content for Project and O&M Deliverables* for Deliverables that are to be maintained during O&M. Include a description of how the Vendor will do the following:

- a. Describe how you will provide ongoing maintenance and support for the Solution. This includes, but is not limited to, periodic updates based on new product versions.
- b. Provide a mechanism for the Agency to request Changes to the Solution and report Defects.
- c. Maintain a tracking system, at no cost to the Agency, to track all requested Changes and reported Defects, their status, expected resolution time, testing results, and final resolution.
- d. Provide the Agency with the status of releases, Changes, and Defect resolution in a format specified by the Agency, O&M Status Reports will contain at a minimum the contents outlined in *Attachment J, Minimum Content for Project and O&M Deliverables*.
- e. Perform technical testing all releases and fixes for Changes and Defects in Vendor's environment prior to delivery to the Agency for UAT. Reference Section 3.5.2.2 for technical testing deliverables.
- f. For modifications made by the Vendor to remediate Defects or make Changes requested by the Agency, Vendor shall provide the Regression Test Results Report to confirm that the Solution has not regressed because of modifications prior to releasing the next version of the Solution for UAT.
- g. Provide the Agency with technical testing results for Changes and Defects as outlined in Section 3.5.2.2 in a format specified by the Agency. Testing results will contain at a minimum the contents outlined in *Attachment J, Minimum Content for Project and O&M Deliverables*.
- h. Upon State request, assist UAT Testers during UAT of any Changes, Defects, and new releases. Vendor will assist the Agency in documenting the UAT Results Report. UAT assistance may be provided onsite or offsite as agreed upon by the Office.
- i. Troubleshoot and correct all problems and Defects identified during UAT of new releases, Defect remediations, or Vendor-assisted Changes to ensure that the Solution continues to operate as designed.

- j. Document Agency Acceptance of Tested Solution prior to deployment of Changes or new releases.
- k. Perform Deployment Validation and document Agency Acceptance of Deployment UAT Results.
- l. The Vendor will troubleshoot browser and other compatibility issues that may develop with new releases, Changes, or new supported browser versions as needed.
- m. Describe the review and update process (annually and when impacted by Changes) for O&M Deliverables listed in Section 3.5.2.2.

2. Vendor Hosting

- a. Describe your development, test, training, production, disaster recovery, and any separate reporting technical hosting environments.
- b. Describe the schedule required to stand up each technical hosting environment.
- c. Describe how Confidential Information will be securely maintained in the Vendor's hosted environment.
- d. Describe how the Vendor will troubleshoot, review, maintain and upgrade all technical environments (servers, operating systems, utility software application software, and SAN storage) as needed to ensure continual compliance/conformance (as applicable) with federal, State, and NCDHHS architectural, privacy, and security policies and standards.
- e. Describe how you will provide 24x7x365 monitoring of the production environment for unusual behavior, error conditions, and hardware, Solution, and operating systems' failures, except during planned or unplanned maintenance periods.
- f. Describe how you will ensure that there is 99.9% uptime Production availability, with unplanned downtime equal to or less than eight (8) hours forty-five (45) minutes and thirty-six (36) seconds annually. Unplanned downtime will be defined in an approved Service Level Agreement (SLA) as indicated in this RFP and resulting Contract.
- i. Indicate whether and describe the Solution supports offline access and data entry if the Internet connection is not available, and how this access can be provided.
- g. Describe how you will maintain the Solution and database backups and perform automated nightly encrypted backups of all the Solution data files with full and incremental methodology.
- h. Describe how you assure a recovery point objective (RPO) of 24 hours and a recovery time objective (RTO) of 72 hours (i.e., maximum down time).
- i. Describe how you will perform disaster recovery testing and the frequency of this testing.
- j. Describe how you will provide, at the request of the Agency, and at no additional cost, a full backup of the Solution data. The data must be accompanied by the following documentation:

- i. Data dictionaries for all tables/databases; and
 - ii. Related reference files and coding guides.
- k. Clearly delineate and maintain the Development, Test, and Production technical hosting environments and a physical separation of hardware, where necessary for security and Change purposes.

3. State Hosting

- a. Describe the development, test, training, production, disaster recovery, and any separate reporting technical hosting environments the State will need to establish and operate to host the Solution.
- b. Describe the schedule required to stand up each technical hosting environment.
- c. Describe how the Vendor will assist the State to troubleshoot, review, maintain and upgrade all technical environments (servers, operating systems, utility software application software, and SAN storage) as needed to ensure continual compliance/conformance (as applicable) with federal, State, and DHHS architectural, privacy, and security policies and standards.
- d. Indicate whether the Solution supports offline access and data entry if the WAN connection is not available.
- e. Describe how you will support the State in performing disaster recovery tasks, including DR testing.

4. Metrics and Performance

- a. Describe how the proposed Solution ensures adequate space on servers, bandwidth, and response time in the Solution to allow for a minimum 690 concurrent users accessing, entering, and reporting information with a capacity to handle up to 1380 with minimal performance degradation.
- b. Describe how the Solution provides capability for transaction response time to be consistent for all users directly interacting with the production environment, based on a common application access for network access point, processed and returned to the network access point:
 - i. Ninety (90) percent of responses to occur in two (2) seconds or less.
 - ii. Ninety-five (95) percent of responses: to occur in three (3) seconds or less.
 - iii. Ninety-seven (97) percent of responses to occur in four (4) seconds or less.
 - iv. Ninety-nine (99) percent of responses to occur in five (5) seconds or less.
- c. Describe your proposed Solution's established performance metrics, and whether it conforms to the response times listed above in b. of this specification. If a separate reporting environment is included in your proposal, please describe the response times for the environment.

5. Vendor Service Level Agreement (SLA)

The Vendor will submit with its RFP response a draft SLA that defines formally the levels of service the Vendor will provide for the Solution during the Project and during O&M and addresses the Agency's service level expectations as listed below. Refer to *Attachment J, Minimum Content for Project and O&M Deliverables* for more information about the expectations of the SLAs contents.

The Agency's service level expectations for the Solution, its availability, and Vendor services are as follows:

- a. Provide 99.9%, 24x7x365 system availability for all calendar days except for any system maintenance windows approved by the Agency.
- b. Provide timely Solution upgrades for fixes and changes in the form of software releases and critical error fixes. Please discuss your support structure including, but not limited to, help desk, problem tracking, maintenance windows and hours of operation.
- c. Provide periodic Solution updates that are provided to all customers at no additional cost to the Office.
- d. Details the process for requesting Changes, tracking the accumulation of Change Request Hours, estimating work hours required for completion, and completing Changes requested by the Agency.
- e. Provide on-going account management and status reporting. If not specified in the SLA included in your offer, describe in your proposal the level of account management provided and any specific services included.
- f. Provide capability for response time to be consistent for all users directly interacting with the Production hosting environment, based on a common Web Portal access for network access point and processed and returned to the network access point according to the response times outlined above in Section 3.5.6.4.
- g. Provide the response, diagnostic and resolution timeframes for problem log entries for the service request categories listed in Section 3.5.6.
- h. Discuss your support for testing performance of the Solution.
- i. Explain the types of reporting that you provide regarding your Solution, including frequency and format (e.g., performance per the SLA, change management, performance/capacity management). Address the types of reporting specified in Section 3.5.2.2.

The draft SLA will be finalized by the Agency prior to Contract award.

During the term of the Contract, Vendor will review and update the SLA each time the SLA is impacted by a request from the Agency to revise service level commitments. During O&M, the SLA will also be subject to periodic review by the Agency's Contract Administrator.

6. Help Desk Support

- a. Describe the help desk support you provide and indicate whether the support is available Monday through Friday 7:00 a.m. – 6:00 p.m. ET. Help desk support activity is considered resolution of the following:
 - i. Category 1, 2, or 3 problems;
 - ii. Persistent product instability;
 - iii. Application of advanced tools for intensive research and development to produce a new release to fix the issue reported;
 - iv. Auditing ability unavailable; and
 - v. Escalated application errors.
- b. Describe any extended hours of help desk support available for emergency response.
- c. Describe additional methods users or the Agency can use to request support (e.g., Internet mechanisms, e-mail, FAX, phone (voicemail)) and response times proposed.

7. Acquisition, Licensing, and Product Overview

- a. Describe all licensing options and licenses terms for your software, including Third-Party software if used as part of your Solution. **The Third-Party Software License Agreements are to be included in the Vendor's offer.**
- b. Explain how your company gathers change feedback from customers and involves them in the prioritization of future releases. Describe how your company measures its ability to satisfy customers' needs.
- c. Discuss how many customers are using the current release of the software. Provide a summary of customer size, industry segment, countries operating in, and applications implemented. Also, indicate for the above, details on transaction volumes, time taken for implementation, the average duration a customer has used the product.
- d. Describe your schedule for new releases, including the next scheduled release for your proposed Solution, detailing how often you provide upgrades, patches or bug fixes to your product; how the customer is notified; and once a new release is made public, how long the previous release is supported.
- e. Describe your procedure for the distribution of upgrades/new releases, modifications, Changes and corresponding documentation.
- f. Discuss the largest implementation you have currently installed (include the number of users, locations and the amount of content stored).
- g. If applicable, provide the name and address of your recommended implementation partner who would support implementation of your products, and the role it would play in the implementation.
- h. Explain whether you have a customer advisory board or user group. If yes, include a list of the present members and explain how often (per year) this organization meets and average meeting duration.

4.0 COST OF VENDOR'S OFFER

4.1 OFFER COSTS

The Vendor must list, itemize, and describe any applicable offer costs which may include the following:

- a) Software License fees or costs to accommodate user base identified.
- b) Additional modules required or proposed addressing specifications, if any.
- c) Third-party software, if any, required for the operation of the Solution.
- d) Installation/configuration/integration/transition costs.
- e) Customization required or proposed addressing specifications: The costs for customization shall be detailed on an attachment by item and cost for each customization to the Vendor product
- f) Conversion and migration of legacy data.
- g) Deliverables in accordance with Section 3.5.2 Table 1: Project Execution and/or O&M Deliverables and Responsibilities, and *Attachment J: Minimum Content for Project and O&M Deliverables*, including updates and revisions.
- h) Training and training materials.
- i) Annual maintenance and Vendor hosting costs per contract year, if not included in Software License Costs.
- j) Customer Support to include Help Desk and Technical Support costs per contract year, if not included in annual maintenance costs or Software License Costs.
- k) Escrow costs (If COTS products are included in the Solution).
- l) Cost of Change Hours per year.
- m) Other costs shall be listed separately by type of service/cost as an attachment. List separately any changes associated with State hosting. Travel and lodging expenses, if any, must be thoroughly described, and are limited by the State's Terms and Conditions.
- n) Hourly rate for additional professional services such as consulting and other value-added services provided the Vendor upon request by the Division.

4.2 PAYMENT SCHEDULE

The Vendor shall propose its itemized payment schedule based on the content of its offer. All payments must be based upon acceptance of one or more Deliverables.

5.0 EVALUATION

5.1 SOURCE SELECTION

A trade-off/ranking method of source selection will be utilized in this procurement to allow the State to award this RFP to the Vendor providing the Best Value and recognizing that Best Value may result in award other than the lowest price or highest technically qualified offer. By using this method, the overall ranking may be adjusted up or down when considered with or traded-off against other non-price factors.

- a) Evaluation Process Explanation. State Agency employees will review all offers. All offers will be initially classified as being responsive or non-responsive. If an offer is found non-responsive, it will not be considered further. All responsive offers will be evaluated based on stated evaluation criteria. Any references in an answer to another location in the RFP materials or Offer shall have specific page numbers and sections stated in the reference.
- b) To be eligible for consideration, Vendor's offer must substantially conform to the intent of all specifications. Compliance with the intent of all specifications will be determined by the State. Offers that do not meet the full intent of all specifications listed in this RFP may be deemed deficient. Further, a serious deficiency in the offer to any one (1) factor may be grounds for rejection regardless of overall score.
- c) The evaluation committee may request clarifications, an interview with or presentation from any or all Vendors as allowed by 9 NCAC 06B.0307. However, the State may refuse to accept, in full or partially, the response to a clarification request given by any Vendor. Vendors are cautioned that the evaluators are not required to request clarifications; therefore, all offers should be complete and reflect the most favorable terms. Vendors should be prepared to send qualified personnel to Raleigh, North Carolina, to discuss technical and contractual aspects of the offer.
- d) Vendors are advised that the State is not obligated to ask for or accept after the closing date for receipt of offer, data that is essential for a complete and thorough evaluation of the offer.

5.2 EVALUATION CRITERIA

Evaluation shall include best value, as the term is defined in N.C.G.S. § 143-135.9(a)(1), compliance with information technology project management policies as defined by N.C.G.S. §143B-1340, compliance with information technology security standards and policies, substantial conformity with the specifications, and other conditions set forth in the solicitation. The following Evaluation Criteria are listed in Order of Importance.

- 1. How well the Vendor's offer conforms with the specifications
- 2. How each Vendor's offer compares with other Vendors' offers
- 3. Total Cost of Ownership
- 4. Illustration(s) and/or explanations of adherence to Section 3.3 Enterprise Specifications
- 5. Vendor Schedule / Timeline for completing work
- 6. Strength of references relevant or material to technology area(s) or Specifications
- 7. Vendor Past Performance - The Vendor may be disqualified from any evaluation or award if the Vendor or any key personnel proposed, has previously failed to perform satisfactorily during the performance of any contract with the State, or violated rules or statutes applicable to public bidding in the State.
- 8. Risks associated with Vendor's offer.

5.3 BEST AND FINAL OFFERS (BAFO)

The State may establish a competitive range based upon evaluations of offers, and request BAFOs from the Vendor(s) within this range, e.g., "Finalist Vendor(s)". If negotiations or subsequent offers are solicited, the Vendor(s) shall provide BAFO(s) in response. Failure to deliver a BAFO when requested shall disqualify the non-responsive Vendor from further consideration. The State will

evaluate BAFO(s), oral presentations, and product demonstrations as part of the Vendors' respective offers to determine the final rankings.

5.4 POSSESSION AND REVIEW

During the evaluation period and prior to award, possession of the bids and accompanying information is limited to personnel of the issuing agency, and to the committee responsible for participating in the evaluation. Vendors who attempt to gain this privileged information, or to influence the evaluation process (i.e., assist in evaluation) will be in violation of purchasing rules and their offer will not be further evaluated or considered.

After award of contract the complete bid file will be available to any interested persons with the exception of trade secrets, test information or similar proprietary information as provided by statute and rule. Any proprietary or confidential information which conforms to exclusions from public records as provided by N.C.G.S. §132-1.2 must be clearly marked as such in the offer when submitted.

6.0 VENDOR INFORMATION AND INSTRUCTIONS

6.1 GENERAL CONDITIONS OF OFFER

6.1.1 VENDOR RESPONSIBILITY

It shall be the Vendor's responsibility to read this entire document, review all enclosures and attachments, and comply with all specifications, requirements and the State's intent as specified herein. If a Vendor discovers an inconsistency, error or omission in this solicitation, the Vendor should request a clarification from the State's contact person.

The Vendor will be responsible for investigating and recommending the most effective and efficient solution. Consideration shall be given to the stability of the proposed configuration and the future direction of technology, confirming to the best of their ability that the recommended approach is not short lived. Several approaches may exist for hardware configurations, other products and any software. The Vendor must provide a justification for their proposed hardware, product and software solution(s) along with costs thereof. Vendors are encouraged to present explanations of benefits and merits of their proposed solutions together with any accompanying Services, maintenance, warranties, value added Services or other criteria identified herein.

6.1.2 RIGHTS RESERVED

While the State has every intention to award a contract as a result of this RFP, issuance of the RFP in no way constitutes a commitment by the State of North Carolina, or the procuring Agency, to award a contract. Upon determining that any of the following would be in its best interests, the State may:

- a) waive any formality;
- b) amend the solicitation;
- c) cancel or terminate this RFP;
- d) reject any or all offers received in response to this RFP;
- e) waive any undesirable, inconsequential, or inconsistent provisions of this RFP;
- f) if the response to this solicitation demonstrates a lack of competition, negotiate directly with one or more Vendors;

- g) not award, or if awarded, terminate any contract if the State determines adequate State funds are not available; or
- h) if all offers are found non-responsive, determine whether Waiver of Competition criteria may be satisfied, and if so, negotiate with one or more known sources of supply.

6.1.3 SOLICITATION AMENDMENTS OR REVISIONS

Any and all amendments or revisions to this document shall be made by written addendum from the Agency Procurement Office. If either a unit price or extended price is obviously in error and the other is obviously correct, the incorrect price will be disregarded.

6.1.4 ORAL EXPLANATIONS

The State will not be bound by oral explanations or instructions given at any time during the bidding process or after award. Vendor contact regarding this RFP with anyone other than the State's contact person may be grounds for rejection of said Vendor's offer. Agency contact regarding this RFP with any Vendor may be grounds for cancellation of this RFP.

6.1.5 E-PROCUREMENT

This is not an E-Procurement solicitation. Attachment B, subparagraphs #38(a) and 38(b) of the attached North Carolina Department of Information Technology Terms and Conditions Services for General Purchases do not apply to this solicitation.

6.1.6 INTERACTIVE PURCHASING SYSTEM (IPS)

The State has implemented links to the Interactive Purchasing System (IPS) that allow the public to retrieve offer award information electronically from our Internet website: <https://www.ips.state.nc.us/ips/>. Click on the IPS BIDS icon, click on Search for BID, enter the Agency prefix-offer number 30-23189-DCDEE, and then search. This information may not be available for several weeks depending upon the complexity of the acquisition and the length of time to complete the evaluation process.

6.1.7 PROTEST PROCEDURES

Protests of awards exceeding \$25,000 in value must be submitted to the issuing Agency at the address given on the first page of this document. Protests must be received in the purchasing Agency's office within fifteen (15) calendar days from the date of this RFP award and provide specific reasons and any supporting documentation for the protest. **All protests are governed by Title 9, Department of Information Technology (formerly Agency of Information Technology Services), Subchapter 06B Sections .1101 - .1121.**

6.2 GENERAL INSTRUCTIONS FOR VENDOR

6.2.1 SITE VISIT OR PRE-OFFER CONFERENCE (RESERVED)

6.2.2 QUESTIONS CONCERNING THE RFP

All inquiries regarding the solicitation specifications or requirements are to be addressed to the contact person listed on Page One of this solicitation via the Ariba Sourcing Tool's message board. Vendor contact regarding this Solicitation with anyone other than the contact person listed on Page One of this Solicitation may be grounds for rejection of said Vendor's offer.

Written questions concerning this Solicitation will be received until **July 10, 2023, at 12:00 pm Eastern Time.**

They must be submitted to the contact person listed on Page One of this Solicitation via Procurement.Questions@dhhs.nc.gov. Please enter "Questions Solicitation 23189" as the subject for the message. Questions should be submitted in the following format:

REFERENCE	VENDOR QUESTION
RFP Section, Page Number	

6.2.3 ADDENDUM TO RFP

If a pre-offer conference is held or written questions are received prior to the submission date, an addendum comprising questions submitted and responses to such questions, or any additional terms deemed necessary by the State shall become an Addendum to this RFP and provided via the State's Ariba Sourcing Tool. Vendors' questions posed orally at any pre-offer conference must be reduced to writing by the Vendor and provided to the Purchasing Officer as directed by said Officer. Oral answers are not binding on the State.

Critical updated information may be included in this Addenda. It is important that all Vendors bidding on this RFP periodically check the State's Ariba Sourcing Tool for any and all Addenda that may be issued prior to the offer opening date.

6.2.4 COSTS RELATED TO OFFER SUBMISSION

Costs for developing and delivering responses to this RFP and any subsequent presentations of the offer as requested by the State are entirely the responsibility of the Vendor. The State is not liable for any expense incurred by the Vendors in the preparation and presentation of their offers.

All materials submitted in response to this RFP become the property of the State and are to be appended to any formal documentation, which would further define or expand any contractual relationship between the State and the Vendor resulting from this RFP process.

6.2.5 VENDOR ERRATA AND EXCEPTIONS

Any errata or exceptions to the State's requirements and specifications may be presented on a separate page labeled "Exceptions to Requirements and Specifications". Include references to the corresponding requirements and specifications of the Solicitation. Any deviations shall be explained in detail. **The Vendor shall not construe this paragraph as inviting deviation or implying that any deviation will be acceptable. Offers of alternative or non-equivalent goods or services may be rejected if not found substantially conforming; and if offered, must be supported by independent documentary verification that the offer substantially conforms to the specified goods or services specification.** If a vendor materially deviates from RFP requirements or specifications, its offer may be determined to be non-responsive by the State.

Offers conditioned upon acceptance of Vendor Errata or Exceptions may be determined to be non-responsive by the State.

6.2.6 ALTERNATE OFFERS

The Vendor may submit alternate offers for various levels of service(s) or products meeting specifications. Alternate offers must specifically identify the RFP specifications and advantage(s)

addressed by the alternate offer. Any alternate offers must be clearly marked with the legend as shown herein. Each offer must be for a specific set of Services or products and offer at specific pricing. If a Vendor chooses to respond with various service or product offerings, each must be an offer with a different price and a separate RFP offer. Vendors may also provide multiple offers for software or systems coupled with support and maintenance options, provided, however, all offers must satisfy the specifications.

Alternate offers must be submitted in a separate document and clearly marked "Alternate Offer for 'name of Vendor'" and numbered sequentially with the first offer if separate offers are submitted.

6.2.7 MODIFICATIONS TO OFFER

An offer may not be unilaterally modified by the Vendor.

6.2.8 BASIS FOR REJECTION

Pursuant to 9 NCAC 06B.0401, the State reserves the right to reject any and all offers, in whole or in part; by deeming the offer unsatisfactory as to quality or quantity, delivery, price or service offered; non-compliance with the specifications or intent of this solicitation; lack of competitiveness; error(s) in specifications or indications that revision would be advantageous to the State; cancellation or other changes in the intended project, or other determination that the proposed specification is no longer needed; limitation or lack of available funds; circumstances that prevent determination of the best offer; or any other determination that rejection would be in the best interest of the State.

6.2.9 NON-RESPONSIVE OFFERS

Vendor offers will be deemed non-responsive by the State and will be rejected without further consideration or evaluation if statements such as the following are included:

- a) "This offer does not constitute a binding offer",
- b) "This offer will be valid only if this offer is selected as a finalist or in the competitive range",
- c) "The Vendor does not commit or bind itself to any terms and conditions by this submission",
- d) "This document and all associated documents are non-binding and shall be used for discussion purposes only",
- e) "This offer will not be binding on either party until incorporated in a definitive agreement signed by authorized representatives of both parties", or
- f) A statement of similar intent

6.2.10 VENDOR REGISTRATION WITH THE SECRETARY OF STATE

Vendors do not have to be registered with the NC Secretary of State to submit an offer; however, in order to receive an award/contract with the State, they must be registered. Registration can be completed at the following website: https://www.sosnc.gov/Guides/launching_a_business

6.2.11 VENDOR REGISTRATION AND SOLICITATION NOTIFICATION SYSTEM

The NC electronic Vendor Portal (eVP) allows Vendors to electronically register with the State to receive electronic notification of current procurement opportunities for goods and Services available on the Interactive Purchasing System at the following website: <https://www.ips.state.nc.us/ips/>.

This RFP is available electronically on the Interactive Purchasing System at <https://www.ips.state.nc.us/ips/>.

6.2.12 VENDOR POINTS OF CONTACT

CONTACTS AFTER CONTRACT AWARD:

Below are the Vendor Points of Contact to be used after award of the contract.

VENDOR CONTRACTUAL POINT OF CONTACT	VENDOR TECHNICAL POINT OF CONTACT
[NAME OF VENDOR] [STREET ADDRESS] [CITY, STATE, ZIP] Attn: Assigned Contract Manager	[NAME OF VENDOR] [STREET ADDRESS] [CITY, STATE, ZIP] Attn: Assigned Technical Lead

6.3 INSTRUCTIONS FOR OFFER SUBMISSION

6.3.1 GENERAL INSTRUCTIONS FOR OFFER

Vendors are strongly encouraged to adhere to the following general instructions in order to bring clarity and order to the offer and subsequent evaluation process:

- Organize the offer in the exact order in which the specifications are presented in the RFP. The Execution page of this RFP must be placed at the front of the Proposal. Each page should be numbered. The offer should contain a table of contents, which cross-references the RFP specification and the specific page of the response in the Vendor's offer.
- Provide complete and comprehensive responses with a corresponding emphasis on being concise and clear. Elaborate offers in the form of brochures or other presentations beyond that necessary to present a complete and effective offer are not desired.
- Clearly state your understanding of the problem(s) presented by this RFP including your proposed solution's ability to meet the specifications, including capabilities, features, and limitations, as described herein, and provide a cost offer.
- Supply all relevant and material information relating to the Vendor's organization, personnel, and experience that substantiates its qualifications and capabilities to perform the Services and/or provide the goods described in this RFP. If relevant and material information is not provided, the offer may be rejected from consideration and evaluation.
- Furnish all information requested; and if response spaces are provided in this document, the Vendor shall furnish said information in the spaces provided. Further, if required elsewhere in this RFP, each Vendor must submit with its offer sketches, descriptive literature and/or complete specifications covering the products offered. References to literature submitted with a previous offer will not satisfy this provision. Proposals that do not comply with these instructions may be rejected.
- Any offer that does not adhere to these instructions may be deemed non-responsive and rejected on that basis.

- g) **Only information that is received in response to this RFP will be evaluated.** Reference to information previously submitted or Internet Website Addresses (URLs) will not suffice as a response to this solicitation.

6.3.2 OFFER ORGANIZATION

Within each section of its offer, Vendor should address the items in the order in which they appear in this RFP. Forms, or attachments or exhibits, if any provided in the RFP, must be completed and included in the appropriate section of the offer. All discussion of offered costs, rates, or expenses must be presented in Section 4.0. Cost of Vendor's Offer.

The offer should be organized and indexed in the following format and should contain, at a minimum, all listed items below.

- a) Signed Execution Page
- b) Table of Contents
- c) Description of Vendor Submitting Offer Form (Attachment D)
- d) Vendor Response to Specifications and Requirements
- e) Security Vendor Readiness Assessment Report (VRAR)
- f) Architecture Diagrams
- g) Cost Form for Vendor's Offer (Attachment E)
- h) Schedule of Offered Solution
- i) Signed Vendor Certification Form (Attachment F)
- j) Location of Workers Utilized by Vendor Form (Attachment G)
- k) References (Attachment H)
- l) Financial Statements (Attachment I)
- m) Errata and Exceptions, if any
- n) Vendor's License and Maintenance Agreements, if any, and Third-Party License Agreements, if any.
- o) Supporting material such as technical system documentation, training examples, etc.
- p) Vendor may attach other supporting materials that it feels may improve the quality of its response. These materials should be included as items in a separate appendix.
- q) All pages of this solicitation document (including Attachments A, B, and C).
- r) Draft Project Management Plan, draft Project Schedule, draft Staffing Plan, draft Service Level Agreement, and draft Vendor Operations and Maintenance Phase Staffing Plan. Please refer to Attachment J: Minimum Content for Project and O&M Deliverables.

6.3.3 OFFER SUBMITTAL

IMPORTANT NOTE: Vendor shall bear the risk for late submission due to unintended or unanticipated delay—whether submitted electronically, delivered by hand, U.S. Postal Service, courier, or other delivery service. **Vendor must include all the pages of this solicitation in their**

response. It is the Vendor's sole responsibility to ensure its offer has been delivered to this Agency by the specified time and date of opening. Any proposal delivered after the proposal deadline will be rejected.

Sealed offers, subject to the conditions made a part hereof, will be received until 2:00pm Eastern Time on the day of opening and then opened, for furnishing and delivering the commodity as described herein. Offers must be submitted via the Ariba Sourcing Module with the Execution page signed and dated by an official authorized to bind the Vendor's firm. Failure to return a signed offer shall result in disqualification.

Attempts to submit a proposal via facsimile (FAX) machine, telephone, or email in response to this Bid shall NOT be accepted.

- a) All File names should start with the Vendor name first, in order to easily determine all the files to be included as part of the vendor's response. For example, files should be named as follows: Vendor Name-your file name.
- b) File contents **SHALL NOT** be password protected, the file formats must be in .PDF, .JPEG, .DOC or .XLS format, and shall be capable of being copied to other sources. Inability by the State to open the Vendor's files may result in the Vendor's offer(s) being rejected.
- c) If the vendor's proposal contains any confidential information (as defined in Attachment B, Section 2, Paragraph #17), then the vendor must provide one (1) signed, original electronic offer and one (1) redacted electronic copy.

7.0 OTHER REQUIREMENTS AND SPECIAL TERMS

7.1 VENDOR UTILIZATION OF WORKERS OUTSIDE OF U.S.

In accordance with N.C.G.S. §143B-1361(b), the Vendor must detail the manner in which it intends to utilize resources or workers in the RFP response. The State of North Carolina will evaluate the additional risks, costs, and other factors associated with such utilization prior to making an award for any such Vendor's offer.

Complete ATTACHMENT G - Location of Workers Utilized by Vendor and submit with your offer.

7.2 FINANCIAL STATEMENTS

The Vendor shall provide evidence of financial stability by returning with its offer 1) completed Financial Review Form (Attachment I), and 2) copies of Financial Statements as further described hereinbelow. As used herein, Financial Statements shall exclude tax returns and compiled statements.

- a) For a publicly traded company, Financial Statements for the past three (3) fiscal years, including at a minimum, income statements, balance sheets, and statement of changes in financial position or cash flows. If three (3) years of financial statements are not available, this information shall be provided to the fullest extent possible, but not less than one year. If less than 3 years, the Vendor must explain the reason why they are not available.
- b) For a privately held company, when certified audited financial statements are not prepared: a written statement from the company's certified public accountant stating the financial condition, debt-to-asset ratio for the past three (3) years and any pending actions that may affect the company's financial condition.

- c) The State may, in its sole discretion, accept evidence of financial stability other than Financial Statements for the purpose of evaluating Vendors' responses to this RFP. The State reserves the right to determine whether the substitute information meets the requirements for Financial Information sufficiently to allow the State to evaluate the sufficiency of financial resources and the ability of the business to sustain performance of this RFP award. Scope Statements issued may require the submission of Financial Statements and specify the number of years to be provided, the information to be provided, and the most recent date required.

7.3 FINANCIAL RESOURCES ASSESSMENT, QUALITY ASSURANCE, PERFORMANCE AND RELIABILITY

- a) Contract Performance Security. The State reserves the right to require performance guaranties pursuant to N.C.G.S. §143B-1340(f) and 09 NCAC 06B.1207 from the Vendor without expense to the State.
- b) Project Assurance, Performance and Reliability Evaluation – Pursuant to N.C.G.S. §143B-1340, the State CIO may require quality assurance reviews of Projects as necessary.

7.4 VENDOR'S LICENSE OR SUPPORT AGREEMENTS

Vendor should present its license or support agreements for review and evaluation. Terms offered for licensing and support of Vendors' proprietary assets will be considered.

The terms and conditions of the Vendor's standard services, license, maintenance or other agreement(s) applicable to Services, Software and other Products acquired under this RFP may apply to the extent such terms and conditions do not materially change the terms and conditions of this RFP. In the event of any conflict between the terms and conditions of this RFP and the Vendor's standard agreement(s), the terms and conditions of this RFP relating to audit and records, jurisdiction, choice of law, the State's electronic procurement application of law or administrative rules, the remedy for intellectual property infringement and the exclusive remedies and limitation of liability in the DIT Terms and Conditions herein shall apply in all cases and supersede any provisions contained in the Vendor's relevant standard agreement or any other agreement. The State shall not be obligated under any standard license and/or maintenance or other Vendor agreement(s) to indemnify or hold harmless the Vendor, its licensors, successors or assigns, nor arbitrate any dispute, nor pay late fees, penalties, legal fees or other similar costs.

7.5 RESELLERS (RESERVE)

7.6 DISCLOSURE OF LITIGATION

The Vendor's failure to fully and timely comply with the terms of this section, including providing reasonable assurances satisfactory to the State, may constitute a material breach of the Agreement.

- a) The Vendor shall notify the State in its offer, if it, or any of its subcontractors, or their officers, directors, or key personnel who may provide Services under any contract awarded pursuant to this solicitation, have ever been convicted of a felony, or any crime involving moral turpitude, including, but not limited to fraud, misappropriation, or deception. The Vendor shall promptly notify the State of any criminal litigation, investigations or proceeding involving the Vendor or any subcontractor, or any of the foregoing entities' then current officers or directors during the term of the Agreement or any Scope Statement awarded to the Vendor.

- b) The Vendor shall notify the State in its offer, and promptly thereafter as otherwise applicable, of any civil litigation, arbitration, proceeding, or judgments against it or its subcontractors during the three (3) years preceding its offer, or which may occur during the term of any awarded to the Vendor pursuant to this solicitation, that involve (1) Services or related goods similar to those provided pursuant to any contract and that involve a claim that may affect the viability or financial stability of the Vendor, or (2) a claim or written allegation of fraud by the Vendor or any subcontractor hereunder, arising out of their business activities, or (3) a claim or written allegation that the Vendor or any subcontractor hereunder violated any federal, state or local statute, regulation or ordinance. Multiple lawsuits and or judgments against the Vendor or subcontractor shall be disclosed to the State to the extent they affect the financial solvency and integrity of the Vendor or subcontractor.
- c) All notices under subsection A and B herein shall be provided in writing to the State within thirty (30) calendar days after the Vendor learns about any such criminal or civil matters; unless such matters are governed by the DIT Terms and Conditions annexed to the solicitation. Details of settlements which are prevented from disclosure by the terms of the settlement shall be annotated as such. Vendor may rely on good faith certifications of its subcontractors addressing the foregoing, which certifications shall be available for inspection at the option of the State.

7.7 CRIMINAL CONVICTION

In the event the Vendor, an officer of the Vendor, or an owner of a 25% or greater share of the Vendor, is convicted of a criminal offense incident to the application for or performance of a State, public or private Contract or subcontract; or convicted of a criminal offense including but not limited to any of the following: embezzlement, theft, forgery, bribery, falsification or destruction of records, receiving stolen property, attempting to influence a public employee to breach the ethical conduct standards for State of North Carolina employees; convicted under State or federal antitrust statutes; or convicted of any other criminal offense which in the sole discretion of the State, reflects upon the Vendor's business integrity and such vendor shall be prohibited from entering into a contract for goods or Services with any department, institution or agency of the State.

7.8 SECURITY AND BACKGROUND CHECKS

The Agency reserves the right to conduct a security background check or otherwise approve any employee or agent provided by the Vendor, and to refuse access to or require replacement of any such personnel for cause, including, but not limited to, technical or training qualifications, quality of work or change in security status or non-compliance with the Agency's security or other similar requirements.

All State and Vendor personnel that have access to data restricted by the State Security Manual and Policies must have a security background check performed. The Vendors are responsible for performing all background checks of their workforce and subcontractors. The State reserves the right to check for non-compliance.

7.9 ASSURANCES

In the event that criminal or civil investigation, litigation, arbitration or other proceedings disclosed to the State pursuant to this Section, or of which the State otherwise becomes aware, during the term of the Agreement, causes the State to be reasonably concerned about:

- a) the ability of the Vendor or its subcontractor to continue to perform the Agreement in accordance with its terms and conditions, or

- b) whether the Vendor or its subcontractor in performing Services is engaged in conduct which is similar in nature to conduct alleged in such investigation, litigation, arbitration or other proceedings, which conduct would constitute a breach of the Agreement or violation of law, regulation or public policy, then the Vendor shall be required to provide the State all reasonable assurances requested by the State to demonstrate that: the Vendor or its subcontractors hereunder will be able to continue to perform the Agreement in accordance with its terms and conditions, and the Vendor or its subcontractors will not engage in conduct in performing Services under the Agreement which is similar in nature to the conduct alleged in any such litigation, arbitration or other proceedings.

7.10 CONFIDENTIALITY OF OFFERS

All offers and any other RFP responses shall be made public as required by the NC Public Records Act and GS 143B-1350. Vendors may mark portions of offers as confidential or proprietary, after determining that such information is excepted from the NC Public Records Act, provided that such marking is clear and unambiguous and preferably at the top and bottom of each page containing confidential information. Standard restrictive legends appearing on every page of an offer are not sufficient and shall not be binding upon the State.

Certain State information is not public under the NC Public Records Act and other laws. Any such information which the State designates as confidential and makes available to the Vendor in order to respond to the RFP or carry out the Agreement, or which becomes available to the Vendor in carrying out the Agreement, shall be protected by the Vendor from unauthorized use and disclosure. The Vendor shall not be required under the provisions of this section to keep confidential, (1) information generally available to the public, (2) information released by the State generally, or to the Vendor without restriction, (3) information independently developed or acquired by the Vendor or its personnel without reliance in any way on otherwise protected information of the State. Notwithstanding the foregoing restrictions, the Vendor and its personnel may use and disclose any information which it is otherwise required by law to disclose, but in each case only after the State has been so notified, and has had the opportunity, if possible, to obtain reasonable protection for such information in connection with such disclosure.

7.11 PROJECT MANAGEMENT

All project management and coordination on behalf of the Agency shall be through a single point of contact designated as the Agency Project Manager. The Vendor shall designate a Vendor Project Manager who will provide a single point of contact for management and coordination of the Vendor's work. All work performed pursuant to the Agreement shall be coordinated between the Agency Project Manager and the Vendor Project Manager.

7.12 MEETINGS

The Vendor is required to meet with Agency personnel, or designated representatives, to resolve technical or contractual problems that may occur during the term of the Agreement. Meetings will occur as problems arise and will be coordinated by the Agency. The Vendor will be given reasonable and sufficient notice of meeting dates, times, and locations. Face-to-face meetings are desired unless noted below. However, at the Vendor's option and expense, a conference call meeting may be substituted. Failure to participate in two (2) consecutive problem resolution meetings, two (2) consecutive missed or rescheduled meetings, or failure to make a good faith effort to resolve problems, may result in termination of the Contract in accordance with Attachment B: Section 1, subsection 19. Default.

The appropriate Vendor Staff will be required to participate in the following project meetings. The DHHS Project Manager will provide 24-hour meeting notice for project meetings. Project meetings specified as “Onsite” require attendance in person in Raleigh, North Carolina or a designated Facility as needed unless public health measures require virtual meetings (e.g., NC DHHS’s COVID-19 pandemic plan response is still active). Project meetings specified as “Offsite” will be conducted via teleconference/Microsoft Teams, or Cisco WebEx.

- a) Project Kick-Off (Onsite)
- b) System Requirements/User Story/Use Case/Backlog Development, Gap Analysis and Detailed Design (Onsite)
- c) Configured State Technical Environments (if the Division selects a State-hosting option) (Onsite or Offsite as warranted by the context and scope of the individual meetings)
- d) Pre-UAT Training (Onsite)
- e) UAT Support (Onsite or Offsite as warranted by the context and scope of the individual meetings)
- f) Role-Based Training for testers, end users, State Administrators, State trainers, and IT support personnel training (Onsite/Offsite, including on demand training such as e-Learning)
- g) Readiness for Deployment (Go-Live) (Onsite)
- h) Deployment (Onsite)
- i) Project Closeout (Offsite)
- j) Ad Hoc Meetings (Onsite/Offsite)
- k) Change Management Meetings (Onsite/Offsite)
- l) Project Review Meetings (Onsite/Offsite)
- m) Executive Steering Committee (Onsite/Offsite)
- n) Project Status Meetings (Onsite/Offsite)

The Project Status Meetings will follow an agenda mutually developed by Vendor and the DHHS Project Manager and will contain the minimum content requirements as described in *Attachment J: Minimum Content for Project and O&M Deliverables*. The Vendor Project Manager will work with the DHHS Project Manager to plan, strategize, and prepare required materials for all the meetings.

When required to be onsite, the Vendor will provide Vendor personnel with any required personal computer equipment and software and will reimburse the Agency for all long-distance telephone calls charged to the Agency.

7.13 RECYCLING AND SOURCE REDUCTION

It is the policy of this State to encourage and promote the purchase of products with recycled content to the extent economically practicable, and to purchase items which are reusable, refillable, repairable, more durable, and less toxic to the extent that the purchase or use is practicable and cost-effective. We also encourage and promote using minimal packaging and the use of recycled/recyclable products in the packaging of goods purchased. However, no sacrifice in quality of packaging will be acceptable. The Vendor remains responsible for providing packaging that will protect the commodity and contain it for its intended use. Vendors are strongly urged to bring to the attention of the purchasers at the NCDIT

Statewide IT Procurement Agency those products or packaging they offer which have recycled content and that are recyclable.

7.14 INVOICES

- a) The State Contractual Point of Contact (i.e., Division Contract Administrator) will be responsible for receiving and tracking statements of completed Deliverables and invoices, and for verifying information and costs submitted in invoices.
- b) Project Deliverables must be grouped in accordance with Solution development and delivery and must be completed and accepted by the Division before the Vendor is eligible to invoice for payment.
- c) Invoices must bear the correct Contract number and purchase order number to ensure prompt payment. Vendor's failure to include the correct purchase order number may cause delay in payment.
- d) Invoices must include an accurate description of the work, identifying the specific Sprint Cycles/Modules/Milestones and Deliverables for which the invoice is being submitted, the invoice date, the period of time covered, the amount of fees due to Vendor and the original signature of the Vendor's Project Manager.
- e) Invoices for O&M will be submitted monthly by the Vendor for the O&M services provided in the prior month and must include penalty adjustments for any Vendor non-performance per the terms of the Service Level Agreement or the penalties listed in Section 3.5.6 Categories of Defects/issues identified during the Stabilization Period.

7.15 SPECIAL TERMS AND CONDITIONS (RESERVED)

ATTACHMENT A: DEFINITIONS

- 1) **24x7:** A statement of availability of systems, communications, and/or supporting resources every hour (24) of each day (7 days weekly) throughout every year for periods specified herein. Where reasonable downtime is accepted, it will be stated herein. Otherwise, 24x7 implies NO loss of availability of systems, communications, and/or supporting resources.
- 2) **ABCMS:** Automated Background Check Management System (ABCMS) which has been developed for use by licensed providers who are required to conduct criminal background checks.
- 3) **Ad-hoc Reports:** Ad hoc reporting is a business intelligence process used to quickly create reports on an as-needed basis. Ad hoc reports are generally created for one-time use to find the answer to a specific business question.
- 4) **Agency:** Division of Child Development and Early Education (DCDEE).
- 5) **Agency Contract Administrator:** The person authorized by the Division of Child Development and Early Education to make day-to-day contract decisions and oversee the contract.
- 6) **Agency Project Manager:** All project management and coordination on behalf of the Agency is through a single point of contact designated as the Agency Project Manager.
- 7) **Agile Software Development:** Refers to a group of software development methodologies based on iterative development, where requirements and solutions evolve through collaboration between self-organizing cross-functional teams.
- 8) **Annual Compliance:** Visit made to a facility within a twelve-month time period by a childcare consultant to monitor for compliance with all applicable childcare requirements.
- 9) **Annual Compliance with Rated License Assessment:** Visit made to monitor compliance with all minimum childcare requirements and applicable enhanced requirements for a Rated License Assessment. (Completed if an annual compliance visit has not been conducted within the last 6 months.)
- 10) **Audit log:** An audit log, also called an audit trail, is essentially a record of events and changes. IT devices across the network create logs based on events. Audit logs are records of these event logs, typically regarding a sequence of activities or a specific activity, they capture events by recording who performed an activity, what activity was performed, and how the system responded.
- 11) **BAFO:** Best and Final Offer.
- 12) **Business Associate Agreement (BAA):** A legally binding document guided by HIPAA rules for signing this agreement before sharing any Protected Health Information (PHI).
- 13) **CBC:** The North Carolina Child Care Law requires a criminal background check (CBC) be conducted and a determination of fitness be made on all persons who work or provide childcare in a licensed or regulated childcare facility.
- 14) **CCSA:** Child Care Service Association (CCSA) improves the quality of childcare in North Carolina for all children by helping families find childcare, offering informational events for families, professional development opportunities and programs for providers and comprehensive childcare research for policymakers.
- 15) **Change:** For the purposes of this RFP, the term Change means the process of modifying the Solution and/or a component of the Solution, whether by Customization or Configuration for the purpose of increasing or decreasing functionality and capability of the Solution or by correcting/resolving Defects or other issues affecting the operation of the Solution. The definition of

the term Change shall not be based on the time and/or size of the effort required to provide such services.

- 16) Change Hours:** Four hundred (400) hours provided by Vendor to the State during Contract Year 1 and two hundred (200) hours for each subsequent Contract Year of the awarded Contract, to be used by the State to obtain Changes to the Solution or Supplemental Support Services at no additional cost. Any of the Change Hours allocated, but unused, during the respective Contract Year, will be rolled over into following Contract Year.
- 17) Change Management:** The processes to be employed by the Division and Vendor to ensure that Changes are captured, planned, and implemented in a visible, controlled, and orderly fashion during the Project Execution and the O&M parts of the Contract. (See Section 7.14 for further information.)
- 18) Change Request (CR):** Changes to the Solution or scope of services will be requested, documented and controlled in forms and logs as outlined in the Change Management process(es).
- 19) Child Care Center:** An arrangement where, at any one time, there are three or more preschool-age children or nine or more school-age children receiving childcare. This does not include arrangements described in Item (18) of the Child Care Rule regarding Family Child Care Homes.
- 20) Child Care Facility:** Includes childcare centers and family childcare homes, and any other childcare arrangement not excluded by N.C.G.S. 110-86(2) that provides childcare.
- 21) Child Care Consultant:** DCDEE employs childcare consultants to ensure childcare regulations are being met. Childcare consultants conduct various visits to programs.
- 22) Child Care Provider:** "Childcare providers" are the following employees who have contact with the children in a childcare program: facility directors, childcare administrative staff, teachers, teachers' aides, substitute providers, uncompensated providers, cooks, maintenance personnel and drivers.
- 23) Child Maltreatment Registry:** The CMR is a list of individuals who have maltreated a child in childcare since the January 2016 Session Law 2015-123 took effect.
- 24) Clearing Houses:** Clearing houses provides educational reporting, verification, and research services to North American colleges and universities.
- 25) Client Services Data Warehouse (CSDW):** a data warehouse accessed by clients via query tools that stores transactional and summarized information from multiple source systems.
- 26) Configurable:** Capable of being configured; customizable; permitting rearrangement or adjustment.
- 27) Customization:** 1) Development of functionality within the Base Product requested by the State to address the specific needs of the State; or 2) Development of functionality outside the Base Product requested by the State to address the specific needs of the State. A Customization is not a Configuration. Customizations must be maintained by Vendor to ensure compatibility with all future Product Upgrades and releases of the Base Product. For the solution to be a considered COTS solution by the Division, the total amount of Customization must not exceed 10% of the base Solution.
- 28) Cybersecurity Incident (GS 143B-1320):** An occurrence that:
 - a. Actually, or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or
 - b. Constitutes a violation or imminent threat of violation of law, security policies, privacy policies, security procedures, or acceptable use policies.

- 29) Defect:** A Defect is an error in coding or logic that causes a program to malfunction or to produce incorrect or unexpected results.
- 30) Defect and Release Management:** Defect and Release Management is the plan and process governing the identification and triage of a Defect to classify, assign, remediate and regression test, assemble and manage the quality of the software release that contains the Defect/s. Traceability entries document Defects found in the Solution, reporting, and recurrence.
- 31) Deliverables:** Deliverables, as used herein, shall comprise all Hardware, Vendor Services, professional Services, Software and provided modifications to any Software, and incidental materials, including any goods, Software or Services access license, data, reports and documentation provided or created during the performance or provision of Services hereunder. Deliverables include “Work Product” and means any expression of Licensor’s findings, analyses, conclusions, opinions, recommendations, ideas, techniques, know-how, designs, programs, enhancements, and other technical information, but not source and object code or software.
- 32) Early Childcare (EC) Workforce:** The EC workforce is made up of individuals working in a variety of settings who serve children prior to kindergarten including home and center-based childcare, private Pre-K, Head Start and Early Head Start and public Pre-K within those programs. Individuals may be program administrators, lead teachers, assistant teachers, or aides.
- 33) Environment Rating Scale:** A tool that is used by an assessor to measure how well caregivers respond to and provide care for children. The Environment Rating Scale (ERS) also assesses health and safety practices. The quality and quantity of play and learning activities are also assessed.
- 34) Executive Steering Committee (ESC):** The governance body responsible for providing direction and oversight to the project, The ESC provides a stabilizing influence with a visionary view. The committee ensures business objectives are met and the project remains under control.
- 35) Facility Administrators/Directors:** Facility administrators/directors supervise and lead staffs, design program plans, oversee daily activities, and prepare budgets. They are responsible for all aspects of their center's program, which may include before- and after-school care.
- 36) Facility Owner:** Facility Owner is the person or entity held legally responsible for the childcare business. An owner is defined as any person with a 5% or greater equity interest in a childcare facility.
- 37) Family Child Care Home (FCCH):** An arrangement located in a residence where, at any one time, more than two children, but less than nine children, receive childcare. Family childcare home operators must reside at the location of the family childcare home.
- 38) FERPA:** Family Educational Rights and Privacy Act
- 39) Frequently Asked Questions (FAQs):** A convenient location within a document to collect common questions which a user might pose along with the appropriate answers and references.
- 40) Goods:** Includes intangibles such as computer software; provided, however that this definition does not modify the definition of “goods” in the context of N.C.G.S. §25-2-105 (UCC definition of goods).
- 41) Go-Live:** The time at which a software Solution becomes available for end users. At this point, all users should have access to the agreed feature set without any restrictions. Prior to going live, the project will complete a project Go-Live readiness assessment based on State and DHHS project management methodology/practices.
- 42) Help Desk:** A service providing information and support to computer users.
- 43) HIPAA:** The Health Insurance Portability and Accountability Act of 1996 and all subsequent acts that updated HIPAA requirements such as the Health Information Technology for Economic and Clinical

Health (HITECH) Act passed as part of the American Recovery and Reinvestment Act of 2009 (ARRA).

- 44) ID:** Identifier (or key) used by a software solution to locate and report on a particular record or piece of electronic information.
- 45) Identify and Access Management (IAM):** Used to administer user identities, roles and access control rights. IAM provides a mechanism to allow users to have access to the appropriate Information Technology (IT) resources and nothing more, based on their role.
- 46) Investigation Consultant:** DCDEE employs investigation consultants to conduct investigations of child maltreatment in childcare facilities, to ensure childcare regulations are being met.
- 47) License Number:** Every home and center has an Identification Number (ID) that is assigned by the Division of Child Development and Early Education. The ID# is listed on the permit (license) or Notice of Compliance. If you have a question about a program, or want to receive information about a program, it is very helpful to have the ID# available when you call or write to the Division of Child Development and Early Education.
- 48) Local Education Agency (LEA):** Local educational agency or LEA means a public board of education or other public authority legally constituted within a State for either administrative control or direction of, or to perform a service function for, public elementary schools or secondary schools in a city, county, township, school district, or other political subdivision of a State, or for a combination of school districts or counties as are recognized in a State as an administrative agency for its public elementary schools or secondary schools. (<https://www.ed.gov/race-top/district-competition/definitions>)
- 49) LEA License & Salary Info Center (LicSal):** Part of the North Carolina Department of Instruction's (NC DPI's) enhanced Salary Administration System that provides LEAs access to key Salary Administration System information.
- 50) Licensure Only Plan:** A plan issued to a teacher candidate with a BA/BS degree who is not employed in a teaching position. A Licensure Only Plan is written by a four-year college or university outlining courses and requirements that must be successfully completed to attain teacher licensure.
- 51) Multi-Factor Authentication (MFA):** An authentication method which requires a user to provide two or more verification factors to gain access to sensitive information or systems.
- 52) Notice of Action (Administrative Action):** Programs that have serious or repeated violations may receive an Administrative Action issued by the Division of Child Development and Early Education. Providers have the right to appeal an Administrative Action. When a provider appeals an action, a contested case hearing before an Administrative Law Judge is scheduled. The hearing is an opportunity for the provider and the Division of Child Development and Early Education to have witnesses testify about the situation which resulted in the Administrative Action. The provider/operator has 30 days after receiving the Notice of Administrative Action to file an appeal.
- 53) NCDHHS:** The North Carolina Department of Health and Human Services
- 54) NCID:** North Carolina Identity Management. The State's standard identity and access management platform from the N.C. Department of Information Technology.
- 55) NCICDP:** North Carolina Institute for Child Development Professionals (NCICDP) provides high quality professional development opportunities to the ECE Workforce. Professional development, in this context, refers to a combination of education and continuing education via college courses, continuing education units, conferences and professional forums as well as workshops along with coaching and mentoring opportunities.

- 56) NCRLAP:** The North Carolina Rated License Assessment Project (NCRLAP) is a collaborative project between the North Carolina Division of Child Development and Early Education (NCDCEE) and other institutions of higher education across the State. NCRLAP's purpose is to conduct voluntary environmental rating scale (ERS) assessments of childcare centers and homes attempting to earn three or more stars within the North Carolina Star Rated License system.
- 57) NIST 800-53 Controls:** The National Institute of Standards and Technology publication known as NIST 800-53 outlines security controls for federal information systems and provides documentation for standards required for all federal information systems, except for those designed for national security.
- 58) Offsite:** Meetings and team collaboration are conducted via teleconference meetings (e.g., Microsoft Teams or Cisco WebEx).
- 59) Onsite:** Requires attendance in person in Raleigh, North Carolina or designated facility as needed unless public health measures require virtual meetings (e.g., NCDHHS's COVID- 19 pandemic plan response is still active).
- 60) Operations and Maintenance (O&M) Contract Phase:** Operations and Maintenance is the process of supporting the Stabilized production Solution and/or components of the Solution to correct defects and maintain performance of the Solution. The definition of Operations and Maintenance shall not be based on the time and/or size of the effort required to provide such services. For the purposes of this RFP and resulting Contract, Operations and Maintenance and the O&M Contract Phase shall also include implementation of Changes that are required by federal or state statutes, regulations and/or rule changes, and reporting requirements. For purposes of this RFP and resulting Contract, the O&M Contract Phase will begin on the first State business day after the Vendor successfully completes the Stabilization Period.
- 61) Out-of-State Providers:** Out-of-State providers are those located more than 40 miles outside of the borders of North Carolina. Border providers are those providers who render services within 40 miles of the North Carolina border.
- 62) Project Execution Contract Phase (or Project Execution Phase):** During the Project Execution Contract Phase, the Vendor will perform the Solution development activities outlined in this RFP. Activities include the full project lifecycle, including, but not limited to, identifying detailed requirements, performing gap analysis, building the Solution to meet the Agency's requirements and specifications, communication to stakeholders; technical testing, training, assuring Agency acceptance of the delivered Solution, deploying the Solution for production use, and Stabilizing the Solution. For more information reference Section 3.7.1-3.7.5. The Project Execution Contract Phase does not include activities that are considered part of the Operations and Maintenance (O&M) Contract Phase.
- 63) Quality Point:** Childcare facilities may choose to meet additional criteria to earn one quality point which will be added to the total points earned in program standards and staff education to determine the total number of stars earned.
- 64) Quality Rating and Improvement System (QRIS):** a systemic approach to assess, improve, and communicate the level of quality in early and school-age care and education programs
- 65) Rated License Assessment:** Visit made to monitor for enhanced licensing requirements for the issuance of a Rated License. (Completed if annual compliance visit has been completed within the last six months.)

- 66) Regional Assistance Licensing Centers (RALC):** There are four Regional Assistance Licensing Centers (RALCs) in North Carolina, created by the NC State Board of Education and the Department of Public Instruction. The centers evaluate provisionally licensed teachers' applications, prescribe courses of study, and outline other requirements needed in order to receive full professional educators' licenses. Upon completion of individuals' plans of study, the RALC will make recommendation to the Licensure Section at DPI for clear licenses.
- 67) Reasonable, Necessary or Proper:** as used herein shall be interpreted solely by the State of North Carolina.
- 68) Residency License:** According to § 115C.270.20.a.5, the Residency License is a one-year license that is renewable twice and has replaced the Lateral Entry License. This is the current alternative pathway to be issued a teaching license in North Carolina.
- 69) RPO:** The Recovery Point Objective is the maximum targeted period in which data might be lost from an IT service due to a major incident or disaster. It is calculated backward from the time of occurrence of the incident.
- 70) RTO:** The Recovery Time Objective is the targeted duration of time and a service level within which a business process must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in business continuity.
- 71) Scribbles:** a document management solution.
- 72) Security Breach:** As defined in N.C.G.S. §75-61.
- 73) Significant Security Incident (GS 143B-1320):** A cybersecurity incident that is likely to result in demonstrable harm to the State's security interests, economy, critical infrastructure, or to the public confidence, civil liberties, or public health and safety of the residents of North Carolina. A significant cybersecurity incident is determined by the following factors:
- a. Incidents that meet thresholds identified by the Department jointly with the Department of Public Safety that involve information:
 - i. That is not releasable to the public and that is restricted or highly restricted according to Statewide Data Classification and Handling Policy; or
 - ii. That involves the exfiltration, modification, deletion, or unauthorized access, or lack of availability to information or systems within certain parameters to include (i) a specific threshold of number of records or users affected as defined in G.S. 75-65 or (ii) any additional data types with required security controls.
 - b. Incidents that involve information that is not recoverable or cannot be recovered within defined timelines required to meet operational commitments defined jointly by the State agency and the Department or can be recovered only through additional measures and has a high or medium functional impact to the mission of an agency.
- 74) SDLC:** The Software Development Life Cycle is a process followed for a software Project, within a software organization. It consists of a detailed plan describing how to develop, maintain, replace, and alter or enhance specific software. The life cycle defines a methodology for improving the quality of software and the overall development process
- 75) Section 508 Compliance:** This indicates compliance with a US federal government law which requires websites to be safe and accessible for people with disabilities. Complete requirements can be found at: www.section508.gov
- 76) SLA:** Service Level Agreement.

- 77) Smart Start:** Smart Start is a statewide initiative to help all North Carolina children enter school healthy and ready to succeed. Smart Start may help with the cost of childcare. It may help childcare homes or centers improve their programs. Smart Start also helps families access health care and other services that are very important during a child's early years.
- 78) Solution Roadmap:** This is a longer-term view of a project which outlines the key milestones and deliverables needed to achieve the overall solution vision.
- 79) Sprint:** For the purposes of this RFP and resulting Contract, the term Sprint means a specific period in the Project Execution when Solution Functionality and/or Deliverables are completed and submitted to the Division for approval.
- 80) Stabilization Period:** For the purposes of this RFP and resulting Contract, the Stabilization Period is an unbroken period of ninety (90) Calendar Days after Statewide deployment and during the Project Execution Contract Phase where: users can successfully log into the Solution; users can perform their daily work without frequent lockups/freezes/shutdowns caused by the Solution; the Solution is routinely available 24x7x365 during the Stabilization Period; and the Solution functions correctly as deployed, with no Severity 1 or Severity 2 defective functionality.
- 81) Stakeholder:** The Stakeholders are the Project business partners and the government agencies at the local and state levels.
- 82) Standard Reports:** Standard Report means a compilation or study developed to display information on selected topics published periodically.
- 83) Star Rated License:** A star rated license is issued based on the evaluation of program standards and staff education. Child Care facilities with a one-star license meet minimum licensing standards. Facilities with a two-to-five-star license voluntarily meet a higher level of enhanced standards.
- 84) State business day:** State business days are Monday through Friday, with the exception of State of North Carolina holidays established by the Office of State Human Resources (reference <https://oshr.nc.gov/state-employee-resources/benefits/leave/holidays>)
- 85) Summer Day Camp:** A center providing care for school-age children exclusively on a seasonal basis between May 15 and September 15. These programs are not required to be licensed unless they participate in the subsidized childcare program.
- 86) System Administrator:** The System Administrator is a State-level administrator for the Solution. The State's System Administrator can grant any location or process to any user account, view any account within User Security, and update any user information.
- 87) Systems and Organization Controls (SOC) 2 Type 2 or Type II:** A vendor certification that indicates a high level of confidence in security, availability, confidentiality and privacy.
- 88) T.E.A.C.H:** The T.E.A.C.H. Early Childhood® Scholarship Program is an umbrella for a variety of different scholarship programs for those working in the early education field in North Carolina. Every TEACH scholarship has 4 components: scholarship, education, compensation, and commitment.
- 89) Technical Assistance (TA):** Technical Assistance (TA) is the provision of targeted and customized supports by a professional(s) with subject matter and adult learning knowledge and skills to develop or strengthen processes, knowledge application, or implementation of services by recipients.
- 90) Technical Support:** A service provided by a hardware or software company which provides registered users with help and advice about their products.
- 91) Third-party:** Relating to a person or group besides the two primarily involved in the situation (for example, third-party service provider, third-party supplier, third-party payer, etc.).

- 92) Total Cost of Ownership (TCO):** The total cost of the contract is defined in Title 9 NCAC 6A . 0102 (28) “as a summation of all purchase, operating, and related costs for the projected lifetime of a good or service”. See Cost Table 3, Attachment E, for significant elements of the Total Cost of Ownership. In addition, the State may incur additional costs based on the Vendor’s proposal (i.e., need to purchase additional/newer equipment to operate the proposed solution, State staff required to complete data conversion or other aspect of the Vendor’s response, etc.) The Total Cost of Ownership will be used to compare costs across bids during the evaluation process.
- 93) User Acceptance Testing (UAT):** Often the final stage of testing for rollout of a software Solution. In this stage, actual users test the software in real-world situations.
- 94) Vendor:** Company, firm, corporation, partnership, individual, etc., submitting an offer in response to a solicitation.
- 95) Vendor Project Manager:** The Vendor designates a Vendor Project Manager who will provide a single point of contact for management and coordination of the Vendor’s work.
- 96) Vendor Readiness Assessment Report (VRAR):** A report that provides information for the State to perform Cybersecurity due diligence when evaluating proposals (and afterward). Refer to the link here: <https://it.nc.gov/documents/vendor-readiness-assessment-report>.
- 97) Vital Records:** NC Vital Records are responsible for recording North Carolina vital events Including: legally registering all births, deaths, fetal deaths, marriages, and divorces which occur in North Carolina, coding vital events for statistical purposes, maintaining vital records and providing certified or uncertified copies to individuals, researchers, and public health programs.
- 98) VMWare:** VMWare, Inc. is a US based company that specializes in cloud computing and computer virtualization. VMWare solutions provide the ability to configure, deploy and manage complex server configurations remotely, without the need for on-site computing hardware.
- 99) Workforce Online Reporting and Knowledge System (WORKS) Application** functions as a single portal of entry for workforce education and professional development to collect, report, and track childcare workforce information needed to support education requirements.
- 100) XML:** Extensible Markup Language. A standard, simple, and widely adopted method of formatting text and data so that it can be exchanged across all of the different computer platforms, languages, and applications.

ATTACHMENT B: DEPARTMENT OF INFORMATION TECHNOLOGY TERMS AND CONDITIONS

Section 1. General Terms and Conditions Applicable to All Purchases

1) **DEFINITIONS:** As used herein;

Agreement means the contract awarded pursuant to this RFP.

Deliverable/Product Warranties shall mean and include the warranties provided for products or deliverables licensed to the State unless superseded by a Vendor's Warranties pursuant to Vendor's License or Support Agreements.

Purchasing State Agency or Agency shall mean the Agency purchasing the goods or Services.

Services shall mean the duties and tasks undertaken by the Vendor to fulfill the requirements and specifications of this solicitation. For a Software as a Service ("SaaS") Solution, Services further include, without limitation, providing web browser access by authorized users to certain Vendor online software applications identified herein, and to related services, such as Vendor hosted Computer storage, databases, Support, documentation, and other functionalities.

State shall mean the State of North Carolina, the Department of Information Technology (DIT), or the Purchasing State Agency in its capacity as the Contracting Agency, as appropriate.

- 2) **STANDARDS:** Any Deliverables shall meet all applicable State and federal requirements, such as State or Federal Regulation, and NC State Chief Information Officer's (CIO) policy or regulation. Vendor will provide and maintain a quality assurance system or program that includes any Deliverables and will tender or provide to the State only those Deliverables that have been inspected and found to conform to the RFP specifications. All Deliverables are subject to operation, certification, testing and inspection, and any accessibility specifications.
- 3) **WARRANTIES:** Unless otherwise expressly provided, any goods Deliverables provided by the Vendor shall be warranted for a period of 90 days after acceptance.
- 4) **SUBCONTRACTING:** The Vendor may subcontract the performance of required Services with Resources under the Agreement only with the prior written consent of the State contracting authority. Vendor shall provide the State with complete copies of any agreements made by and between Vendor and all subcontractors. The selected Vendor remains solely responsible for the performance of its subcontractors. Subcontractors, if any, shall adhere to the same standards required of the selected Vendor and the Agreement. Any contracts made by the Vendor with a subcontractor shall include an affirmative statement that the State is an intended third-party beneficiary of the Agreement; that the subcontractor has no agreement with the State; and that the State shall be indemnified by the Vendor for any claim presented by the subcontractor. Notwithstanding any other term herein, Vendor shall timely exercise its contractual remedies against any non-performing subcontractor and, when appropriate, substitute another subcontractor.
- 5) **TRAVEL EXPENSES:** All travel expenses should be included in the Vendor's proposed costs. Separately stated travel expenses will not be reimbursed. In the event that the Vendor, upon specific request in writing by the State, is deemed eligible to be reimbursed for travel expenses arising under the performance of the Agreement, reimbursement will be at the out-of-state rates set forth in N.C.G.S. §138-6; as amended from time to time. Vendor agrees to use the lowest available airfare not requiring a weekend stay and to use the lowest available rate for rental vehicles. All Vendor incurred travel expenses shall be billed on a monthly basis, shall be supported by receipt and shall be paid by the State within thirty (30) days after invoice approval. Travel expenses exceeding the foregoing rates shall not be paid by the State. The State will reimburse travel allowances only for days on which the Vendor is required to be in North Carolina performing Services under the Agreement.
- 6) **GOVERNMENTAL RESTRICTIONS:** In the event any restrictions are imposed by governmental requirements that necessitate alteration of the material, quality, workmanship, or performance of the

Deliverables offered prior to delivery thereof, the Vendor shall provide written notification of the necessary alteration(s) to the Agency Contract Administrator. The State reserves the right to accept any such alterations, including any price adjustments occasioned thereby, or to cancel the Agreement. The State may advise Vendor of any restrictions or changes in specifications required by North Carolina legislation, rule or regulatory authority that require compliance by the State. In such event, Vendor shall use its best efforts to comply with the required restrictions or changes. If compliance cannot be achieved by the date specified by the State, the State may terminate the Agreement and compensate Vendor for sums then due under the Agreement.

- 7) **PROHIBITION AGAINST CONTINGENT FEES AND GRATUITIES:** Vendor warrants that it has not paid, and agrees not to pay, any bonus, commission, fee, or gratuity to any employee or official of the State for the purpose of obtaining any Contract or award issued by the State. Vendor further warrants that no commission or other payment has been or will be received from or paid to any third-party contingent on the award of any Contract by the State, except as shall have been expressly communicated to the State Purchasing Agent in writing prior to acceptance of the Agreement or award in question. Each individual signing below warrants that he or she is duly authorized by their respective Party to sign the Agreement and bind the Party to the terms and conditions of this RFP. Vendor and their authorized signatory further warrant that no officer or employee of the State has any direct or indirect financial or personal beneficial interest, in the subject matter of the Agreement; obligation or Contract for future award of compensation as an inducement or consideration for making the Agreement. Subsequent discovery by the State of non-compliance with these provisions shall constitute sufficient cause for immediate termination of all outstanding contracts. Violations of this provision may result in debarment of the Vendor(s) as permitted by 9 NCAC 06B..1206, or other provision of law.
- 8) **AVAILABILITY OF FUNDS:** Any and all payments to Vendor are expressly contingent upon and subject to the appropriation, allocation and availability of funds to the Agency for the purposes set forth in the Agreement. If the Agreement or any Purchase Order issued hereunder is funded in whole or in part by federal funds, the Agency's performance and payment shall be subject to and contingent upon the continuing availability of said federal funds for the purposes of the Agreement or Purchase Order. If the term of the Agreement extends into fiscal years subsequent to that in which it is approved, such continuation of the Agreement is expressly contingent upon the appropriation, allocation and availability of funds by the N.C. Legislature for the purposes set forth in this RFP. If funds to effect payment are not available, the Agency will provide written notification to Vendor. If the Agreement is terminated under this paragraph, Vendor agrees to take back any affected Deliverables and software not yet delivered under the Agreement, terminate any Services supplied to the Agency under the Agreement, and relieve the Agency of any further obligation thereof. The State shall remit payment for Deliverables and Services accepted prior to the date of the aforesaid notice in conformance with the payment terms.
- 9) **ACCEPTANCE PROCESS:**
- a) The State shall have the obligation to notify Vendor, in writing ten calendar days following provision, performance (under a provided milestone or otherwise as agreed) or delivery of any Services or other Deliverables described in the Agreement that are not acceptable.
 - b) Acceptance testing is required for all Vendor supplied software and software or platform services unless provided otherwise in the solicitation documents or a Statement of Work. The State may define such processes and procedures as may be necessary or proper, in its opinion and discretion, to ensure compliance with the State's specifications, and Vendor's Product Warranties and technical representations. The State shall have the obligation to notify Vendor, in writing and within thirty (30) days following installation of any software deliverable if it is not acceptable.
 - c) Acceptance of Services or other Deliverables including software or platform services may be controlled by an amendment hereto, or additional terms as agreed by the Parties consistent with IT Project management under GS §143B-1340.
 - d) The notice of non-acceptance shall specify in reasonable detail the reason(s) a Service or given Deliverable is unacceptable. Acceptance by the State shall not be unreasonably withheld; but may be conditioned or delayed as required for installation and/or testing of Deliverables. Final acceptance is expressly conditioned upon completion of any applicable inspection and testing procedures. Should

a Service or Deliverable fail to meet any specifications or acceptance criteria, the State may exercise any and all rights hereunder. Services or Deliverables discovered to be defective or failing to conform to the specifications may be rejected upon initial inspection or at any later time if the defects or errors contained in the Services or Deliverables or non-compliance with the specifications were not reasonably ascertainable upon initial inspection. If the Vendor fails to promptly cure or correct the defect or replace or re-perform the Services or Deliverables, the State reserves the right to cancel the Purchase Order, contract with a different Vendor, and to invoice the original Vendor for any differential in price over the original Contract price.

- 10) PAYMENT TERMS:** Monthly Payment terms are Net 30 days after receipt of correct invoice (with completed timesheets for Vendor personnel) and acceptance of one or more of the Deliverables, under milestones or otherwise as may be provided in Paragraph 9 (Acceptance), or elsewhere in this solicitation, unless a period of more than thirty (30) days is required by the Agency. The Purchasing State Agency is responsible for all payments under the Agreement. No additional charges to the Agency will be permitted based upon, or arising from, the Agency's use of a Business Procurement Card. The State may exercise any and all rights of Set Off as permitted in Chapter 105A-1 *et. seq.* of the N.C. General Statutes and applicable Administrative Rules. Upon Vendor's written request of not less than thirty (30) days and approval by the State or Agency, the Agency may:
- a) Forward the Vendor's payment check(s) directly to any person or entity designated by the Vendor, or
 - b) Include any person or entity designated in writing by Vendor as a joint payee on the Vendor's payment check(s), however
 - c) In no event shall such approval and action obligate the State to anyone other than the Vendor and the Vendor shall remain responsible for fulfillment of all Contract obligations.
- 11) EQUAL EMPLOYMENT OPPORTUNITY:** Vendor shall comply with all Federal and State requirements concerning fair employment and employment of the disabled, and concerning the treatment of all employees without regard to discrimination by reason of race, color, religion, sex, national origin or physical disability.
- 12) ADVERTISING/PRESS RELEASE:** The Vendor absolutely shall not publicly disseminate any information concerning the Agreement without prior written approval from the State or its Agent. For the purpose of this provision of the Agreement, the Agent is the Purchasing Agency Contract Administrator unless otherwise named in the solicitation documents.
- 13) LATE DELIVERY:** Vendor shall advise the Agency contact person or office immediately upon determining that any Deliverable will not, or may not, be delivered or performed at the time or place specified. Together with such notice, Vendor shall state the projected delivery time and date. In the event the delay projected by Vendor is unsatisfactory, the Agency shall so advise Vendor and may proceed to procure the particular substitute Services or other Deliverables.
- 14) ACCESS TO PERSONS AND RECORDS:** Pursuant to N.C.G.S. §147-64.7, the Agency, the State Auditor, appropriate federal officials, and their respective authorized employees or agents are authorized to examine all books, records, and accounts of the Vendor insofar as they relate to transactions with any department, board, officer, commission, institution, or other agency of the State of North Carolina pursuant to the performance of the Agreement or to costs charged to the Agreement. The Vendor shall retain any such books, records, and accounts for a minimum of three (3) years after the completion of the Agreement. Additional audit or reporting requirements may be required by any Agency, if in the Agency's opinion, such requirement is imposed by federal or state law or regulation.
- 15) ASSIGNMENT:** Vendor may not assign the Agreement or its obligations hereunder except as permitted by 09 NCAC 06B.1003 and this Paragraph. Vendor shall provide reasonable notice of not less than thirty (30) days prior to any consolidation, acquisition, or merger. Any assignee shall affirm the Agreement attorning and agreeing to the terms and conditions agreed, and that Vendor shall affirm that the assignee is fully capable of performing all obligations of Vendor under the Agreement. An assignment may be made, if at all, in writing by the Vendor, Assignee and the State setting forth the foregoing obligation of Vendor and Assignee.
- 16) INSURANCE COVERAGE:** During the term of the Agreement, the Vendor at its sole cost and expense shall provide commercial insurance of such type and with such terms and limits as may be reasonably

associated with the Agreement. As a minimum, the Vendor shall provide and maintain the following coverage and limits:

- a) **Worker's Compensation** - The Vendor shall provide and maintain Worker's Compensation Insurance, as required by the laws of North Carolina, as well as employer's liability coverage with minimum limits of \$100,000.00, covering all of Vendor's employees who are engaged in any work under the Agreement. If any work is sublet, the Vendor shall require the subcontractor to provide the same coverage for any of his employees engaged in any work under the Agreement; and
- b) **Commercial General Liability** - General Liability Coverage on a Comprehensive Broad Form on an occurrence basis in the minimum amount of \$2,000,000.00 Combined Single Limit (Defense cost shall be in excess of the limit of liability); and
- c) **Automobile** - Automobile Liability Insurance, to include liability coverage, covering all owned, hired and non-owned vehicles, used in connection with the Agreement. The minimum combined single limit shall be \$500,000.00 bodily injury and property damage; \$500,000.00 uninsured/under insured motorist; and \$5,000.00 medical payment; and
- d) Providing and maintaining adequate insurance coverage described herein is a material obligation of the Vendor and is of the essence of the Agreement. All such insurance shall meet all laws of the State of North Carolina. Such insurance coverage shall be obtained from companies that are authorized to provide such coverage and that are authorized by the Commissioner of Insurance to do business in North Carolina. The Vendor shall at all times comply with the terms of such insurance policies, and all requirements of the insurer under any such insurance policies, except as they may conflict with existing North Carolina laws or the Agreement. The limits of coverage under each insurance policy maintained by the Vendor shall not be interpreted as limiting the Vendor's liability and obligations under the Agreement.

17) DISPUTE RESOLUTION: The parties agree that it is in their mutual interest to resolve disputes informally. A claim by the Vendor shall be submitted in writing to the Agency Contract Administrator for decision. A claim by the State shall be submitted in writing to the Vendor's Contract Administrator for decision. The Parties shall negotiate in good faith and use all reasonable efforts to resolve such dispute(s). During the time the Parties are attempting to resolve any dispute, each shall proceed diligently to perform their respective duties and responsibilities under the Agreement. If a dispute cannot be resolved between the Parties within thirty (30) days after delivery of notice, either Party may elect to exercise any other remedies available under the Agreement, or at law. This term shall not constitute an agreement by either party to mediate or arbitrate any dispute.

18) CONFIDENTIALITY: In accordance with N.C.G.S. §143B-1350(e) and 143B-1375, and 09 NCAC 06B.0103 and 06B.1001, the State may maintain the confidentiality of certain types of information described in N.C.G.S. §132-1 *et seq.* Such information may include trade secrets defined by N.C.G.S. §66-152 and other information exempted from the Public Records Act pursuant to N.C.G.S. §132-1.2. Vendor may designate appropriate portions of its response as confidential, consistent with and to the extent permitted under the Statutes and Rules set forth above, by marking the top and bottom of pages containing confidential information with a legend in boldface type "**CONFIDENTIAL**". By so marking any page, the Vendor warrants that it has formed a good faith opinion, having received such necessary or proper review by counsel and other knowledgeable advisors that the portions marked confidential meet the requirements of the Rules and Statutes set forth above. **However, under no circumstances shall price information be designated as confidential.** The State may serve as custodian of Vendor's confidential information and not as an arbiter of claims against Vendor's assertion of confidentiality. If an action is brought pursuant to N.C.G.S. §132-9 to compel the State to disclose information marked confidential, the Vendor agrees that it will intervene in the action through its counsel and participate in defending the State, including any public official(s) or public employee(s). The Vendor agrees that it shall hold the State and any official(s) and individual(s) harmless from any and all damages, costs, and attorneys' fees awarded against the State in the action. The State agrees to promptly notify the Vendor in writing of any action seeking to compel the disclosure of Vendor's confidential information. The State shall have the right, at its option and expense, to participate in the defense of the action through its counsel. The State shall have no liability to Vendor with respect to the disclosure of Vendor's confidential

information ordered by a court of competent jurisdiction pursuant to N.C.G.S. §132-9 or other applicable law.

- a) Care of Information: Vendor agrees to use commercial best efforts to safeguard and protect any data, documents, files, and other materials received from the State or the Agency during performance of any contractual obligation from loss, destruction or erasure. Vendor agrees to abide by all facilities and security requirements and policies of the agency where work is to be performed. Any Vendor personnel shall abide by such facilities and security requirements and shall agree to be bound by the terms and conditions of the Agreement.
- b) Vendor warrants that all its employees and any approved third-party Vendors or subcontractors are subject to a non-disclosure and confidentiality agreement enforceable in North Carolina. Vendor will, upon request of the State, verify and produce true copies of any such agreements. Production of such agreements by Vendor may be made subject to applicable confidentiality, non-disclosure or privacy laws; provided that Vendor produces satisfactory evidence supporting exclusion of such agreements from disclosure under the N.C. Public Records laws in N.C.G.S. §132-1 *et seq.* The State may, in its sole discretion, provide a non-disclosure and confidentiality agreement satisfactory to the State for Vendor's execution. The State may exercise its rights under this subparagraph as necessary or proper, in its discretion, to comply with applicable security regulations or statutes including, but not limited to 26 USC 6103 and IRS Publication 1075, (Tax Information Security Guidelines for Federal, State, and Local Agencies), HIPAA, 42 USC 1320(d) (Health Insurance Portability and Accountability Act), any implementing regulations in the Code of Federal Regulations, and any future regulations imposed upon the Department of Information Technology or the N.C. Department of Revenue pursuant to future statutory or regulatory requirements.
- c) Nondisclosure: Vendor agrees and specifically warrants that it, its officers, directors, principals and employees, and any subcontractors, shall hold all information received during performance of the Agreement in the strictest confidence and shall not disclose the same to any third party without the express written approval of the State.
- d) The Vendor shall protect the confidentiality of all information, data, instruments, studies, reports, records and other materials provided to it by the Agency or maintained or created in accordance with this Agreement. No such information, data, instruments, studies, reports, records and other materials in the possession of Vendor shall be disclosed in any form without the prior written consent of the State Agency. The Vendor will have written policies governing access to and duplication and dissemination of all such information, data, instruments, studies, reports, records and other materials.
- e) All project materials, including software, data, and documentation created during the performance or provision of Services hereunder that are not licensed to the State or are not proprietary to the Vendor are the property of the State of North Carolina and must be kept confidential or returned to the State, or destroyed. Proprietary Vendor materials shall be identified to the State by Vendor prior to use or provision of Services hereunder and shall remain the property of the Vendor. Derivative works of any Vendor proprietary materials prepared or created during the performance of provision of Services hereunder shall be subject to a perpetual, royalty free, nonexclusive license to the State.

19) DEFAULT: In the event Services or other Deliverable furnished or performed by the Vendor during performance of any Contract term fail to conform to any material requirement(s) of the Contract specifications, notice of the failure is provided by the State and if the failure is not cured within ten (10) days, or Vendor fails to meet the requirements of Paragraph 9) herein, the State may cancel the contract. Default may be cause for debarment as provided in 09 NCAC 06B.1206. The rights and remedies of the State provided above shall not be exclusive and are in addition to any other rights and remedies provided by law or under the Contract.

- a) If Vendor fails to deliver or provide correct Services or other Deliverables within the time required by the Agreement, the State shall provide written notice of said failure to Vendor, and by such notice require performance assurance measures pursuant to N.C.G.S. 143B-1340(f). Vendor is responsible for the delays resulting from its failure to deliver or provide services or other Deliverables.
- b) Should the State fail to perform any of its obligations upon which Vendor's performance is conditioned, Vendor shall not be in default for any delay, cost increase or other consequences

resulting from the State's failure. Vendor will use reasonable efforts to mitigate delays, costs or expenses arising from assumptions in the Vendor's offer documents that prove erroneous or are otherwise invalid. Any deadline that is affected by any such failure in assumptions or performance by the State shall be extended by an amount of time reasonably necessary to compensate for the effect of such failure.

- c) Vendor shall provide a plan to cure any delay or default if requested by the State. The plan shall state the nature of the delay or default, the time required for cure, any mitigating factors causing or tending to cause the delay or default, and such other information as the Vendor may deem necessary or proper to provide.
- d) If the prescribed acceptance testing stated in the Solicitation Documents or performed pursuant to Paragraph **Error! Reference source not found.** of the DIT Terms and Conditions is not completed successfully, the State may request substitute Software, cancel the portion of the Contract that relates to the unaccepted Software, or continue the acceptance testing with or without the assistance of Vendor. These options shall remain in effect until such time as the testing is successful or the expiration of any time specified for completion of the testing. If the testing is not completed after exercise of any of the State's options, the State may cancel any portion of the contract related to the failed Software and take action to procure substitute software. If the failed software (or the substituted software) is an integral and critical part of the proper completion of the work for which the Deliverables identified in the solicitation documents or statement of work were acquired, the State may terminate the entire contract.

20) WAIVER OF DEFAULT: Waiver by either party of any default or breach by the other Party shall not be deemed a waiver of any subsequent default or breach and shall not be construed to be a modification or novation of the terms of the Agreement, unless so stated in writing and signed by authorized representatives of the Agency and the Vendor, and made as an amendment to the Agreement pursuant to Paragraph 40) herein below.

21) TERMINATION: Any notice or termination made under the Agreement shall be transmitted via US Mail, Certified Return Receipt Requested. The period of notice for termination shall begin on the day the return receipt is signed and dated.

- a) The parties may mutually terminate the Agreement by written agreement at any time.
- b) The State may terminate the Agreement, in whole or in part, pursuant to Paragraph 19), or pursuant to the Special Terms and Conditions in the Solicitation Documents, if any, or for any of the following:
 - i) Termination for Cause: In the event any goods, software, or service furnished by the Vendor during performance of any Contract term fails to conform to any material requirement of the Contract, and the failure is not cured within the specified time after providing written notice thereof to Vendor, the State may cancel and procure the articles or Services from other sources; holding Vendor liable for any excess costs occasioned thereby, subject only to the limitations provided in Paragraphs 22) and 23) herein. The rights and remedies of the State provided above shall not be exclusive and are in addition to any other rights and remedies provided by law or under the Contract. Vendor shall not be relieved of liability to the State for damages sustained by the State arising from Vendor's breach of the Agreement; and the State may, in its discretion, withhold any payment due as a setoff until such time as the damages are finally determined or as agreed by the parties. Voluntary or involuntary Bankruptcy or receivership by Vendor shall be cause for termination.
 - ii) Termination For Convenience Without Cause: The State may terminate service and indefinite quantity contracts, in whole or in part by giving thirty (30) days prior notice in writing to the Vendor. Vendor shall be entitled to sums due as compensation for Deliverables provided and Services performed in conformance with the Contract. In the event the Contract is terminated for the convenience of the State the Agency will pay for all work performed and products delivered in conformance with the Contract up to the date of termination.
 - iii) Consistent failure to participate in problem resolution meetings, two (2) consecutive missed or rescheduled meetings, or failure to make a good faith effort to resolve problems, may result in termination of the Agreement.

22) LIMITATION OF VENDOR'S LIABILITY:

- a) Where Deliverables are under the State's exclusive management and control, the Vendor shall not be liable for direct damages caused by the State's failure to fulfill any State responsibilities of assuring the proper use, management and supervision of the Deliverables and programs, audit controls, operating methods, office procedures, or for establishing all proper checkpoints necessary for the State's intended use of the Deliverables. Vendor shall not be responsible for any damages that arise from (i) misuse or modification of Vendor's Software by or on behalf of the State, (ii) the State's failure to use corrections or enhancements made available by Vendor, (iii) the quality or integrity of data from other automated or manual systems with which the Vendor's Software interfaces, (iv) errors in or changes to third party software or hardware implemented by the State or a third party (including the vendors of such software or hardware) that is not a subcontractor of Vendor or that is not supported by the Deliverables, or (vi) the operation or use of the Vendor's Software not in accordance with the operating procedures developed for the Vendor's Software or otherwise in a manner not contemplated by this Agreement.
- b) The Vendor's liability for damages to the State arising under the contract shall be limited to two times the value of the Contract.
- c) The foregoing limitation of liability shall not apply to claims covered by other specific provisions including but not limited to Service Level Agreement or Deliverable/Product Warranties, or to claims for injury to persons or damage to tangible personal property, gross negligence or willful or wanton conduct. This limitation of liability does not apply to contributions among joint tortfeasors under N.C.G.S. 1B-1 *et seq.*, the receipt of court costs or attorney's fees that might be awarded by a court in addition to damages after litigation based on the Agreement. For avoidance of doubt, the Parties agree that the Service Level Agreement and Deliverable/Product Warranty Terms in the Contract are intended to provide the sole and exclusive remedies available to the State under the Contract for the Vendor's failure to comply with the requirements stated therein.

23) VENDOR'S LIABILITY FOR INJURY TO PERSONS OR DAMAGE TO PROPERTY:

- a) The Vendor shall be liable for damages arising out of personal injuries and/or damage to real or tangible personal property of the State, employees of the State, persons designated by the State for training, or person(s) other than agents or employees of the Vendor, designated by the State for any purpose, prior to, during, or subsequent to delivery, installation, acceptance, and use of the Deliverables either at the Vendor's site or at the State's place of business, provided that the injury or damage was caused by the fault or negligence of the Vendor.
- b) The Vendor agrees to indemnify, defend and hold the Agency and the State and its Officers, employees, agents and assigns harmless from any liability relating to personal injury or injury to real or personal property of any kind, accruing or resulting to any other person, firm or corporation furnishing or supplying work, Services, materials or supplies in connection with the performance of the Agreement, whether tangible or intangible, arising out of the ordinary negligence, wilful or wanton negligence, or intentional acts of the Vendor, its officers, employees, agents, assigns or subcontractors.
- c) Vendor shall not be liable for damages arising out of or caused by an alteration or an attachment not made or installed by the Vendor.

24) TIME IS OF THE ESSENCE: Time is of the essence in the performance of the Agreement.

25) DATE AND TIME WARRANTY: The Vendor warrants that any Deliverable, whether Services, hardware, firmware, middleware, custom or commercial software, or internal components, subroutines, and interface therein which performs, modifies or affects any date and/or time data recognition function, calculation, or sequencing, will still enable the modified function to perform accurate date/time data and leap year calculations. This warranty shall survive termination or expiration of the Contract.

26) INDEPENDENT CONTRACTORS: Vendor and its employees, officers and executives, and subcontractors, if any, shall be independent Vendors and not employees or agents of the State. The Agreement shall not operate as a joint venture, partnership, trust, agency or any other similar business relationship.

- 27) TRANSPORTATION:** Transportation of any tangible Deliverables shall be FOB Destination; unless otherwise specified in the solicitation document or purchase order. Freight, handling, hazardous material charges, and distribution and installation charges shall be included in the total price of each item. Any additional charges shall not be honored for payment unless authorized in writing by the Purchasing State Agency. In cases where parties, other than the Vendor ship materials against this order, the shipper must be instructed to show the purchase order number on all packages and shipping manifests to ensure proper identification and payment of invoices. A complete packing list must accompany each shipment.
- 28) NOTICES:** Any notices required under the Agreement should be delivered to the Contract Administrator for each party. Unless otherwise specified in the Solicitation Documents, any notices shall be delivered in writing by U.S. Mail, Commercial Courier or by hand.
- 29) TITLES AND HEADINGS:** Titles and Headings in the Agreement are used for convenience only and do not define, limit or proscribe the language of terms identified by such Titles and Headings.
- 30) AMENDMENT:** The Agreement may not be amended orally or by performance. Any amendment must be made in written form and signed by duly authorized representatives of the State and Vendor in conformance with Paragraph 36) herein.
- 31) TAXES:** The State of North Carolina is exempt from Federal excise taxes and no payment will be made for any personal property taxes levied on the Vendor or for any taxes levied on employee wages. Agencies of the State may have additional exemptions or exclusions for federal or state taxes. Evidence of such additional exemptions or exclusions may be provided to Vendor by Agencies, as applicable, during the term of the Agreement. Applicable State or local sales taxes shall be invoiced as a separate item.
- 32) GOVERNING LAWS, JURISDICTION, AND VENUE:**
- a) The Agreement is made under and shall be governed and construed in accordance with the laws of the State of North Carolina and applicable Administrative Rules. The place of the Agreement or purchase order, its situs and forum, shall be Wake County, North Carolina, where all matters, whether sounding in Contract or in tort, relating to its validity, construction, interpretation and enforcement shall be determined. Vendor agrees and submits, solely for matters relating to the Agreement, to the jurisdiction of the courts of the State of North Carolina, and stipulates that Wake County shall be the proper venue for all matters.
 - b) Except to the extent the provisions of the Contract are clearly inconsistent therewith, the applicable provisions of the Uniform Commercial Code as modified and adopted in North Carolina shall govern the Agreement. To the extent the Contract entails both the supply of "goods" and "Services," such shall be deemed "goods" within the meaning of the Uniform Commercial Code, except when deeming such Services as "goods" would result in a clearly unreasonable interpretation.
- 33) FORCE MAJEURE:** Neither party shall be deemed to be in default of its obligations hereunder if and so long as it is prevented from performing such obligations as a result of events beyond its reasonable control, including without limitation, fire, power failures, any act of war, hostile foreign action, nuclear explosion, riot, strikes or failures or refusals to perform under subcontracts, civil insurrection, earthquake, hurricane, tornado, or other catastrophic natural event or act of God.
- 34) COMPLIANCE WITH LAWS:** The Vendor shall comply with all laws, ordinances, codes, rules, regulations, and licensing requirements that are applicable to the conduct of its business, including those of federal, state, and local agencies having jurisdiction and/or authority.
- 35) SEVERABILITY:** In the event that a court of competent jurisdiction holds that a provision or requirement of the Agreement violates any applicable law, each such provision or requirement shall be enforced only to the extent it is not in violation of law or is not otherwise unenforceable and all other provisions and requirements of the Agreement shall remain in full force and effect. All promises, requirement, terms, conditions, provisions, representations, guarantees and warranties contained herein shall survive the expiration or termination date unless specifically provided otherwise herein, or unless superseded by applicable federal or State statute, including statutes of repose or limitation.
- 36) CHANGES:** The Agreement and subsequent purchase order(s) is awarded subject to the provision of the specified Services and the shipment or provision of other Deliverables as specified herein. Any changes made to the Agreement or purchase order proposed by the Vendor are hereby rejected unless

accepted in writing by the Agency or State Award Authority. The State shall not be responsible for Services or other Deliverables delivered without a purchase order from the Agency or State Award Authority.

37) FEDERAL INTELLECTUAL PROPERTY BANKRUPTCY PROTECTION ACT: The Parties agree that the Agency shall be entitled to all rights and benefits of the Federal Intellectual Property Bankruptcy Protection Act, Public Law 100-506, codified at 11 U.S.C. 365(n), and any amendments thereto.

38) ELECTRONIC PROCUREMENT (Applies to all contracts that include E-Procurement and are identified as such in the body of the solicitation document): Purchasing shall be conducted through the Statewide E-Procurement Services. The State's third-party agent shall serve as the Supplier Manager for this E-Procurement Services. The Vendor shall register for the Statewide E-Procurement Services within two (2) business days of notification of award in order to receive an electronic purchase order resulting from award of the Agreement.

- a) **The successful Vendor(s) shall pay a transaction fee of 1.75% (.0175) on the total dollar amount (excluding sales taxes) of each purchase order issued through the Statewide E-Procurement Service.** This applies to all purchase orders, regardless of the quantity or dollar amount of the purchase order. The transaction fee shall neither be charged to nor paid by the State, or by any State approved users of the contract. The transaction fee shall not be stated or included as a separate item in the proposed contract or invoice. There are no additional fees or charges to the Vendor for the Services rendered by the Supplier Manager under the Agreement. Vendor will receive a credit for transaction fees they paid for the purchase of any item(s) if an item(s) is returned through no fault of the Vendor. Transaction fees are non-refundable when an item is rejected and returned, or declined, due to the Vendor's failure to perform or comply with specifications or requirements of the contract.
- b) Vendor, or its authorized Reseller, as applicable, will be invoiced monthly for the State's transaction fee by the Supplier Manager. The transaction fee shall be based on purchase orders issued for the prior month. Unless Supplier Manager receives written notice from the Vendor identifying with specificity any errors in an invoice within thirty (30) days of the receipt of invoice, such invoice shall be deemed to be correct, and Vendor shall have waived its right to later dispute the accuracy and completeness of the invoice. Payment of the transaction fee by the Vendor is due to the account designated by the State within thirty (30) days after receipt of the correct invoice for the transaction fee, which includes payment of all portions of an invoice not in dispute. Within thirty (30) days of the receipt of invoice, Vendor may request in writing an extension of the invoice payment due date for that portion of the transaction fee invoice for which payment of the related goods by the governmental purchasing entity has not been received by the Vendor. If payment of the transaction fee invoice is not received by the State within this payment period, it shall be considered a material breach of contract. The Supplier Manager shall provide, whenever reasonably requested by the Vendor in writing (including electronic documents), supporting documentation from the E-Procurement Service that accounts for the amount of the invoice.
- c) The Supplier Manager will capture the order from the State approved user, including the shipping and payment information, and submit the order in accordance with the E-Procurement Services. Subsequently, the Supplier Manager will send those orders to the appropriate Vendor on State Contract. The State or State approved user, not the Supplier Manager, shall be responsible for the solicitation, offers received, evaluation of offers received, award of Contract, and the payment for goods delivered.
- d) Vendor agrees at all times to maintain the confidentiality of its username and password for the Statewide E-Procurement Services. If a Vendor is a corporation, partnership or other legal entity, then the Vendor may authorize its employees to use its password. Vendor shall be responsible for all activity and all charges for such employees. Vendor agrees not to permit a third party to use the Statewide E-Procurement Services through its account. If there is a breach of security through the Vendor's account, Vendor shall immediately change its password and notify the Supplier Manager of the security breach by e-mail. Vendor shall cooperate with the state and the Supplier Manager to mitigate and correct any security breach.

39) PATENT, COPYRIGHT, AND TRADE SECRET PROTECTION:

- a) Vendor has created, acquired or otherwise has rights in, and may, in connection with the performance of Services for the State, employ, provide, create, acquire or otherwise obtain rights in various concepts, ideas, methods, methodologies, procedures, processes, know-how, techniques, models, templates and general-purpose consulting and software tools, utilities and routines (collectively, the "Vendor technology"). To the extent that any Vendor technology is contained in any of the Services or Deliverables including any derivative works, the Vendor hereby grants the State a royalty-free, fully paid, worldwide, perpetual, non-exclusive license to use such Vendor technology in connection with the Services or Deliverables for the State's purposes.
- b) Vendor shall not acquire any right, title and interest in and to the copyrights for goods, any and all software, technical information, specifications, drawings, records, documentation, data or derivative works thereof, or other work products provided by the State to Vendor. The State hereby grants Vendor a royalty-free, fully paid, worldwide, perpetual, non-exclusive license for Vendor's internal use to non-confidential deliverables first originated and prepared by the Vendor for delivery to the State.
- c) The Vendor, at its own expense, shall defend any action brought against the State to the extent that such action is based upon a claim that the Services or other Deliverables supplied by the Vendor, or the operation of such pursuant to a current version of vendor-supplied software, infringes a patent, or copyright or violates a trade secret in the United States. The Vendor shall pay those costs and damages finally awarded against the State in any such action; damages shall be limited as provided in N.C.G.S. 143B-1350(h1). Such defense and payment shall be conditioned on the following:
 - i. That the Vendor shall be notified within a reasonable time in writing by the State of any such claim; and,
 - ii. That the Vendor shall have the sole control of the defense of any action on such claim and all negotiations for its settlement or compromise, provided, however, that the State shall have the option to participate in such action at its own expense.
- d) Should any Services or other Deliverables supplied by Vendor, or the operation thereof become, or in the Vendor's opinion are likely to become, the subject of a claim of infringement of a patent, copyright, or a trade secret in the United States, the State shall permit the Vendor, at its option and expense, either to procure for the State the right to continue using the Services or Deliverables, or to replace or modify the same to become noninfringing and continue to meet procurement specifications in all material respects. If neither of these options can reasonably be taken, or if the use of such Services or Deliverables by the State shall be prevented by injunction, the Vendor agrees to take back any goods/hardware or software, and refund any sums the State has paid Vendor less any reasonable amount for use or damage and make every reasonable effort to assist the state in procuring substitute Services or Deliverables. If, in the sole opinion of the State, the return of such infringing Services or Deliverables makes the retention of other Services or Deliverables acquired from the Vendor under the agreement impractical, the State shall then have the option of terminating the contract, or applicable portions thereof, without penalty or termination charge. The Vendor agrees to take back Services or Deliverables and refund any sums the State has paid Vendor less any reasonable amount for use or damage.
- e) Vendor will not be required to defend or indemnify the State if any claim by a third party against the State for infringement or misappropriation (i) results from the State's alteration of any Vendor-branded Service or Deliverable, or (ii) results from the continued use of the good(s) or services and other Services or Deliverables after receiving notice they infringe a trade secret of a third party.
- f) Nothing stated herein, however, shall affect Vendor's ownership in or rights to its preexisting intellectual property and proprietary rights.

40) UNANTICIPATED TASKS In the event that additional work must be performed that was wholly unanticipated, and that is not specified in the Agreement, but which in the opinion of both parties is necessary to the successful accomplishment of the contracted scope of work, the procedures outlined in this article will be followed. For each item of unanticipated work, the Vendor shall prepare a work authorization in accordance with the State's practices and procedures.

- a) It is understood and agreed by both parties that all of the terms and conditions of the Agreement shall remain in force with the inclusion of any work authorization. A work authorization shall not constitute a contract separate from the Agreement, nor in any manner amend or supersede any of the other terms or provisions of the Agreement or any amendment hereto.
- b) Each work authorization shall comprise a detailed statement of the purpose, objective, or goals to be undertaken by the Vendor, the job classification or approximate skill level or sets of the personnel required, an identification of all significant material then known to be developed by the Vendor's personnel as a Deliverable, an identification of all significant materials to be delivered by the State to the Vendor's personnel, an estimated time schedule for the provision of the Services by the Vendor, completion criteria for the work to be performed, the name or identification of Vendor's personnel to be assigned, the Vendor's estimated work hours required to accomplish the purpose, objective or goals, the Vendor's billing rates and units billed, and the Vendor's total estimated cost of the work authorization.
- c) All work authorizations must be submitted for review and approval by the procurement office that approved the original Contract and procurement. This submission and approval must be completed prior to execution of any work authorization documentation or performance thereunder. All work authorizations must be written and signed by the Vendor and the State prior to beginning work.
- d) The State has the right to require the Vendor to stop or suspend performance under the "Stop Work" provision of the North Carolina Department of Information Technology Terms and Conditions.
- e) The Vendor shall not expend Personnel resources at any cost to the State in excess of the estimated work hours unless this procedure is followed: If, during performance of the work, the Vendor determines that a work authorization to be performed under the Agreement cannot be accomplished within the estimated work hours, the Vendor will be required to complete the work authorization in full. Upon receipt of such notification, the State may:
 - a. Authorize the Vendor to expend the estimated additional work hours or service in excess of the original estimate necessary to accomplish the work authorization, or
 - b. Terminate the work authorization, or
 - c. Alter the scope of the work authorization in order to define tasks that can be accomplished within the remaining estimated work hours.
 - d. The State will notify the Vendor in writing of its election within seven (7) calendar days after receipt of the Vendor's notification. If notice of the election is given to proceed, the Vendor may expend the estimated additional work hours or Services.

41) STOP WORK ORDER The State may issue a written Stop Work Order to Vendor for cause at any time requiring Vendor to suspend or stop all, or any part, of the performance due under the Agreement for a period up to ninety (90) days after the Stop Work Order is delivered to the Vendor. The ninety (90) day period may be extended for any further period for which the parties may agree.

- a) The Stop Work Order shall be specifically identified as such and shall indicate that it is issued under this term. Upon receipt of the Stop Work Order, the Vendor shall immediately comply with its terms and take all reasonable steps to minimize incurring costs allocable to the work covered by the Stop Work Order during the period of work suspension or stoppage. Within a period of ninety (90) days after a Stop Work Order is delivered to Vendor, or within any extension of that period to which the parties agree, the State shall either:
 - i) Cancel the Stop Work Order, or
 - ii) Terminate the work covered by the Stop Work Order as provided for in the termination for default or the termination for convenience clause of the Agreement.

- b) If a Stop Work Order issued under this clause is canceled or the period of the Stop Work Order or any extension thereof expires, the Vendor shall resume work. The State shall make an equitable adjustment in the delivery schedule, the Agreement price, or both, and the Agreement shall be modified, in writing, accordingly, if:
 - i) The Stop Work Order results in an increase in the time required for, or in the Vendor's cost properly allocable to the performance of any part of the Agreement, and
 - ii) The Vendor asserts its right to an equitable adjustment within thirty (30) days after the end of the period of work stoppage; provided that if the State decides the facts justify the action, the State may receive and act upon an offer submitted at any time before final payment under the Agreement.
- c) If a Stop Work Order is not canceled and the work covered by the Stop Work Order is terminated in accordance with the provision entitled Termination for Convenience of the State, the State shall allow reasonable direct costs resulting from the Stop Work Order in arriving at the termination settlement.
- d) The State shall not be liable to the Vendor for loss of profits because of a Stop Work Order issued under this term.

42) TRANSITION ASSISTANCE Reserved

Section 2: Terms and Conditions Applicable to Software as a Service (SaaS)

1) DEFINITIONS:

- a) "Data" includes and means information, formulae, algorithms, or other content that the State, the State's employees, agents and end users upload, create or modify using the Services pursuant to this Agreement. Data also includes user identification information and metadata which may contain Data or from which the State's Data may be ascertainable.
- b) Reserved.
- c) Reserved.
- d) Reserved.
- e) "Support" includes provision of ongoing updates and maintenance for the Vendor online software applications, and as may be specified herein, consulting, training and other support Services as provided by the Vendor for SaaS tenants receiving similar SaaS Services.

2) ACCESS AND USE OF SAAS SERVICES:

- a) The Vendor grants the State a personal non-transferable and non-exclusive right to use and access, all Services and other functionalities or services provided, furnished or accessible under this Agreement. The State may utilize the Services as agreed herein and in accordance with any mutually agreed Acceptable Use Policy. The State is authorized to access State Data and any Vendor-provided data as specified herein and to transmit revisions, updates, deletions, enhancements, or modifications to the State Data. This shall include the right of the State to, and access to, Support without the Vendor requiring a separate maintenance or support agreement. Subject to an agreed limitation on the number of users, the State may use the Services with any computer, computer system, server, or desktop workstation owned or utilized by the State or other authorized users. User access to the Services shall be routinely provided by the Vendor and may be subject to a more specific Service Level Agreement (SLA) agreed to in writing by the parties. The State shall notify the Vendor of any unauthorized use of any password or account, or any other known or suspected breach of security access. The State also agrees to refrain from taking any steps, such as reverse engineering, reverse assembly or reverse compilation to derive a source code equivalent to the Services or any portion thereof. Use of the Services to perform services for commercial third parties (so-called "service bureau" uses) is not permitted, but the State may utilize the Services to perform its governmental functions. If the Services fees are based upon the number of Users and/or hosted instances, the number of Users/hosted instances available may be adjusted at any

time (subject to the restrictions on the maximum number of Users specified in the Furnish and Deliver Table herein above) by mutual agreement and State Procurement approval. All Services and information designated as “confidential” or “proprietary” shall be kept in confidence except as may be required by the North Carolina Public Records Act: N.C.G.S. § 132-1, *et. seq.*

- b) The State's access license for the Services and its associated services neither transfers, vests, nor infers any title or other ownership right in any intellectual property rights of the Vendor or any third party, nor does this license transfer, vest, or infer any title or other ownership right in any source code associated with the Services unless otherwise agreed to by the parties. The provisions of this paragraph will not be construed as a sale of any ownership rights in the Services. Any Services or technical and business information owned by Vendor or its suppliers or licensors made accessible or furnished to the State shall be and remain the property of the Vendor or such other party, respectively. Vendor has a limited, non-exclusive license to access and use the State Data as provided to Vendor, but solely for performing its obligations under this Agreement and in confidence as provided herein.
- c) The Vendor or its suppliers shall at minimum, and except as otherwise agreed, provide telephone assistance to the State for all Services procured hereunder during the State's normal business hours (unless different hours are specified herein). The Vendor warrants that its Support and customer service and assistance will be performed in accordance with generally accepted industry standards. The State has the right to receive the benefit of upgrades, updates, maintenance releases or other enhancements or modifications made generally available to the Vendor's SaaS tenants for similar Services. The Vendor's right to a new use agreement for new version releases of the Services shall not be abridged by the foregoing. The Vendor may, at no additional charge, modify the Services to improve operation and reliability or to meet legal requirements.
- d) The Vendor will provide to the State the same Services for updating, maintaining and continuing optimal performance for the Services as provided to other similarly situated users or tenants of the Services, but minimally as provided for and specified herein. Unless otherwise agreed in writing, Support will also be provided for any other (e.g., third party) software provided by the Vendor in connection with the Vendor's solution herein. The technical and professional activities required for establishing, managing, and maintaining the Services environment are the responsibilities of the Vendor. Any training specified herein will be provided by the Vendor to certain State users for the fees or costs as set forth herein or in an SLA.
- e) Services provided pursuant to this Solicitation may, in some circumstances, be accompanied by a user clickwrap agreement. The term clickwrap agreement refers to an agreement that requires the end user to manifest his or her assent to terms and conditions by clicking an “ok” or “agree” button on a dialog box or pop-up window as part of the process of access to the Services. All terms and conditions of any clickwrap agreement provided with any Services solicited herein shall have no force and effect and shall be non-binding on the State, its employees, agents, and other authorized users of the Services.
- f) The Vendor may utilize partners and/or subcontractors to assist in the provision of the Services, so long as the State Data is not removed from the United States unless the terms of storage of the State Data are clearly disclosed, the security provisions referenced herein can still be complied with, and such removal is done with the prior express written permission of the State. The Vendor shall identify all of its strategic business partners related to Services provided under this contract including, but not limited to, all subcontractors or other entities or individuals who may be a party to a joint venture or similar agreement with the Vendor, who will be involved in any application development and/or operations.
- g) The Vendor warrants that all Services will be performed with professional care and skill, in a workmanlike manner and in accordance with the Services documentation and this Agreement.
- h) An SLA or other agreed writing shall contain provisions for scalability of Services and any variation in fees or costs as a result of any such scaling.
- i) Professional services provided by the Vendor at the request by the State in writing in addition to agreed Services shall be at the then-existing Vendor hourly rates when provided, unless otherwise agreed in writing by the parties.

3) **WARRANTY OF NON-INFRINGEMENT:**

- a) The Vendor warrants to the best of its knowledge that:
 - i) The Services do not infringe any intellectual property rights of any third party; and

- ii) There are no actual or threatened actions arising from, or alleged under, any intellectual property rights of any third party.

- b) Reserved.
- c) Reserved.
- d) Reserved.

4) **ACCESS AVAILABILITY; REMEDIES:**

- a) The Vendor warrants that the Services will be in good working order, and operating in conformance with Vendor's standard specifications and functions as well as any other specifications agreed to by the parties in writing, and shall remain accessible 24/7, with the exception of scheduled outages for maintenance and of other service level provisions agreed in writing, e.g., in an SLA. The Vendor does not warrant that the operation of the Services will be completely uninterrupted or error free, or that the Services functions will meet all the State's requirements unless developed as Customized Services.
- b) The State shall notify the Vendor if the Services are not in good working order or inaccessible during the term of the Agreement. The Vendor shall, at its option, either repair, replace or reperform any Services reported or discovered as not being in good working order and accessible during the applicable contract term without cost to the State. If the Services' monthly availability averages less than 99.9% (excluding agreed-upon maintenance downtime), the State shall be entitled to receive automatic credits as indicated immediately below, or the State may use other contractual remedies such as recovery of damages, as set forth herein in writing, e.g., in Specifications, Special Terms or in an SLA, and as such other contractual damages are limited by N.C.G.S. § 143B-1350(h1) and the Limitation of Liability paragraph below. If not otherwise provided, the automatic remedies for non-availability of the Subscription Services during a month are:
 - 1. A 10% service credit applied against future fees if Vendor does not reach 99.9% availability.
 - 2. A 25% service credit applied against future fees if Vendor does not reach 99% availability.
 - 3. A 50% service credit applied against future fees or eligibility for early termination of the Agreement if Vendor does not reach 95% availability.

If, however, Services meet the 99.9% service availability level for a month but are not available for a consecutive 120 minutes during that month, the Vendor shall grant to the State a credit of a pro-rated one-day of the monthly subscription Services fee against future Services charges. Such credit(s) shall be applied to the bill immediately following the month in which the Vendor failed to meet the performance requirements or other service levels, and the credit will continue to be deducted from the monthly invoice for each prior month that Vendor fails to meet the support response times for the remainder of the duration of the Agreement. If Services monthly availability averages less than 99.9% (excluding agreed-upon maintenance downtime), for three (3) or more months in a rolling twelve-month period, the State may also terminate the contract for material breach in accordance with the Default provisions hereinbelow.

- c) Support Services. Reserved.

5) **EXCLUSIONS:**

- a) Except as stated above in Paragraphs 3 and 4, Vendor and its parent, subsidiaries and affiliates, subcontractors and suppliers make no warranties, express or implied, as to the Services.
- b) The warranties provided in Paragraphs 3 and 4 above do not cover repair for damages, malfunctions or service failures substantially caused by:
 - i) Actions of non-Vendor personnel;
 - ii) Failure to follow Vendor's written instructions relating to the Services provided to the State; or
 - iii) Force Majeure conditions set forth hereinbelow.
 - iv) The State's sole misuse of, or its own inability to use, the Services.

- 6) **PERFORMANCE REVIEW AND ACCOUNTABILITY:** N.C.G.S. § 143B-1340(f) and 09 NCAC 06B.1207 require provisions for performance review and accountability in State IT contracts. For this procurement, these shall include the holding a retainage of ten percent (10%) of the contract value and withholding the final payment contingent on final acceptance by the State as provided in 09 NCAC 06B.1207(3) and (4), unless waived or otherwise agreed, in writing. The Services herein will be provided consistent with and under these Services performance review and accountability guarantees.

- 7) **LIMITATION OF LIABILITY:** **Limitation of Vendor's Contract Damages Liability:** Reserved.

- 8) **VENDOR'S LIABILITY FOR INJURY TO PERSONS OR DAMAGE TO PROPERTY:** Reserved.
- 9) **MODIFICATION OF SERVICES:** If Vendor modifies or replaces the Services provided to the State and other tenants, and if the State has paid all applicable Subscription Fees, the State shall be entitled to receive, at no additional charge, access to a newer version of the Services that supports substantially the same functionality as the then accessible version of the Services. Newer versions of the Services containing substantially increased functionality may be made available to the State for an additional subscription fee. In the event of either of such modifications, the then accessible version of the Services shall remain fully available to the State until the newer version is provided to the State and accepted. If a modification materially affects the functionality of the Services as used by the State, the State, at its sole option, may defer such modification.
- 10) **TRANSITION PERIOD:**
a) Reserved.
- 11) **TRANSPORTATION:** Transportation charges for any Deliverable sent to the State other than electronically or by download shall be FOB Destination unless delivered by internet or file-transfer as agreed by the State, or otherwise specified in the solicitation document or purchase order.
- 12) **TRAVEL EXPENSES:** Reserved.
- 13) **PROHIBITION AGAINST CONTINGENT FEES AND GRATUITIES:** Reserved.
- 14) **AVAILABILITY OF FUNDS:** Reserved.
- 15) **PAYMENT TERMS (Applicable to SaaS):**
a) Payment may be made by the State in advance of or in anticipation of subscription Services to be actually performed under the Agreement or upon proper invoice for other Services rendered. Payment terms are Net 30 days after receipt of correct invoice. Initial payments are to be made after final acceptance of the Services. Payments are subject to any retainage requirements herein. The Purchasing State Agency is responsible for all payments under the Agreement. Subscription fees for term years after the initial year shall be as quoted under State options herein but shall not increase more than five percent (5%) over the prior term, except as the parties may have agreed to an alternate formula to determine such increases in writing. No additional charges to the State will be permitted based upon, or arising from, the State's use of a Business Procurement Card. The State may exercise any and all rights of Set Off as permitted in Chapter 105A-1 *et seq.* of the N.C. General Statutes and applicable Administrative Rules.
- b) Upon the Vendor's written request of not less than thirty (30) days and approval by the State, the State may:
i) Forward the Vendor's payment check(s) directly to any person or entity designated by the Vendor or
ii) Include any person or entity designated in writing by Vendor as a joint payee on the Vendor's payment check(s), however,
iii) In no event shall such approval and action obligate the State to anyone other than the Vendor and the Vendor shall remain responsible for fulfillment of all Agreement obligations.
- c) For any third-party software licensed by the Vendor or its subcontractors for use by the State, a copy of the software license including terms acceptable to the State, an assignment acceptable to the State, and documentation of license fees paid by the Vendor must be provided to the State before any related license fees or costs may be billed to the State.
- d) An undisputed invoice is an invoice for which the State and/or the Purchasing State Agency has not disputed in writing within thirty (30) days from the invoice date, unless the agency requests more time for review of the invoice. Upon the Vendor's receipt of a disputed invoice notice, the Vendor will work to correct the applicable invoice error, provided that such dispute notice shall not relieve the State or the applicable Purchasing State Agency from its payment obligations for the undisputed items on the invoice or for any disputed items that are ultimately corrected. The Purchasing State Agency is not required to pay the Vendor for any Software or Services provided without a written purchase order from the appropriate Purchasing State Agency. In addition, all such Services provided must meet all terms, conditions, and specifications of this Agreement and purchase order and be accepted as satisfactory by the Purchasing State Agency before payment will be issued.
- e) The Purchasing State Agency shall release any amounts held as retainages for Services completed within a reasonable period after the end of the period(s) or term(s) for which the retainage was withheld.

Payment retainage shall apply to all invoiced items, excepting only such items as the Vendor obtains from Third Parties and for which costs are chargeable to the State by agreement of the Parties. The Purchasing State Agency, in its sole discretion, may release retainages withheld from any invoice upon acceptance of the Services identified or associated with such invoices.

16) **ACCEPTANCE CRITERIA:** Reserved.

17) **CONFIDENTIALITY:** Reserved.

18) **SECURITY OF STATE DATA:**

- a) All materials, including software, Data, information and documentation provided by the State to the Vendor (State Data) during the performance or provision of Services hereunder are the property of the State of North Carolina and must be kept secure and returned to the State. The Vendor will protect State Data in its hands from unauthorized disclosure, loss, damage, destruction by natural event, or other eventuality. Proprietary Vendor materials shall be identified to the State by the Vendor prior to use or provision of Services hereunder and shall remain the property of the Vendor. Derivative works of any Vendor proprietary materials prepared or created during the performance or provision of Services hereunder shall be provided to the State as part of the Services. The Vendor shall not access State User accounts, or State Data, except (i) during data center operations; (ii) in response to service or technical issues; (iii) as required by the express terms of this contract; or (iv) at the State's written request. The Vendor shall protect the confidentiality of all information, Data, instruments, studies, reports, records and other materials provided to it by the State or maintained or created in accordance with this Agreement. No such information, Data, instruments, studies, reports, records and other materials in the possession of Vendor shall be disclosed in any form without the prior written agreement with the State. The Vendor will have written policies governing access to and duplication and dissemination of all such information, Data, instruments, studies, reports, records and other materials.
- b) The Vendor shall not store or transfer non-public State data outside of the United States. This includes backup data and Disaster Recovery locations. The Service Provider will permit its personnel and contractors to access State of North Carolina data remotely only as required to provide technical support.
- c) Protection of personal privacy and sensitive data. The Vendor acknowledges its responsibility for securing any restricted or highly restricted data, as defined by the Statewide Data Classification and Handling Policy (<https://it.nc.gov/document/statewide-data-classification-and-handling-policy>) that is collected by the State and stored in any Vendor site or other Vendor housing systems including, but not limited to, computer systems, networks, servers, or databases, maintained by Vendor or its agents or subcontractors in connection with the provision of the Services. The Vendor warrants, at its sole cost and expense, that it shall implement processes and maintain the security of data classified as restricted or highly restricted; provide reasonable care and efforts to detect fraudulent activity involving the data; and promptly notify the State of any breaches of security within twenty-four (24) hours of confirmation as required by N.C.G.S. § 143B-1379.
- d) The Vendor will provide and maintain secure backup of the State Data. The Vendor shall implement and maintain secure passwords for its online system providing the Services, as well as all appropriate administrative, physical, technical and procedural safeguards at all times during the term of this Agreement to secure such Data from Data Breach, protect the Data and the Services from loss, corruption, unauthorized disclosure, and the introduction of viruses, disabling devices, malware and other forms of malicious or inadvertent acts that can disrupt the State's access to its Data and the Services. The Vendor will allow periodic back-up of State Data by the State to the State's infrastructure as the State requires or as may be provided by law.
- e) The Vendor shall certify to the State:
 - i) The sufficiency of its security standards, tools, technologies and procedures in providing Services under this Agreement;
 - ii) That the system used to provide the Subscription Services under this Contract has and will maintain a valid third-party security certification not to exceed one (1) year and is consistent with the data classification level and a security controls appropriate for low or moderate information system(s) per the National Institute of Standards and Technology NIST 800-53 revision 4. The State reserves the right to independently evaluate, audit, and verify such requirements.

iii) That the Services will comply with the following:

- (1) Any DIT security policy regarding Cloud Computing, and the DIT Statewide Information Security Policy Manual; to include encryption requirements as defined below:
 - (a) The Vendor shall encrypt all non-public data in transit regardless of the transit mechanism.
 - (b) For engagements where the Vendor stores sensitive personally identifiable or otherwise confidential information, this data shall be encrypted at rest. Examples are social security number, date of birth, driver's license number, financial data, federal/state tax information, and hashed passwords. The Vendor's encryption shall be consistent with validated cryptography standards as specified in National Institute of Standards and Technology FIPS140-2, Security Requirements. The key location and other key management details will be discussed and negotiated by both parties. When the Service Provider cannot offer encryption at rest, it must maintain, for the duration of the contract, cyber security liability insurance coverage for any loss resulting from a data breach. Additionally, where encryption of data at rest is not possible, the Vendor must describe existing security measures that provide a similar level of protection;
 - (2) Privacy provisions of the Federal Privacy Act of 1974;
 - (3) The North Carolina Identity Theft Protection Act, N.C.G.S. Chapter 75, Article 2A (e.g., N.C.G.S. § 75-65 and -66);
 - (4) The North Carolina Public Records Act, N.C.G.S. Chapter 132;
 - (5) Applicable Federal, State and industry standards and guidelines including, but not limited to, relevant security provisions of the Payment Card Industry (PCI) Data Security Standard (PCIDSS) including the PCIDSS Cloud Computing Guidelines, Criminal Justice Information, The Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA); and
 - (6) Any requirements implemented by the State under N.C.G.S. §§ 143B-1376 and -1377.
 - (7) Any requirements implemented by the State under N.C.G.S. § 20-309.2(d).
- f) Security Breach. "Security Breach" under the NC Identity Theft Protection Act (N.C.G.S. § 75-60ff) means (1) any circumstance pursuant to which applicable Law requires notification of such breach to be given to affected parties or other activity in response to such circumstance (e.g., N.C.G.S. § 75-65); or (2) any actual, attempted, suspected, threatened, or reasonably foreseeable circumstance that compromises, or could reasonably be expected to compromise, either Physical Security or Systems Security (as such terms are defined below) in a fashion that either does or could reasonably be expected to permit unauthorized Processing (as defined below), use, disclosure or acquisition of or access to any the State Data or state confidential information. "Physical Security" means physical security at any site or other location housing systems maintained by Vendor or its agents or subcontractors in connection with the Services. "Systems Security" means security of computer, electronic or telecommunications systems of any variety (including data bases, hardware, software, storage, switching and interconnection devices and mechanisms), and networks of which such systems are a part or communicate with, used directly or indirectly by Vendor or its agents or subcontractors in connection with the Services. "Processing" means any operation or set of operations performed upon the State Data or State confidential information, whether by automatic means, such as creating, collecting, procuring, obtaining, accessing, recording, organizing, storing, adapting, altering, retrieving, consulting, using, disclosing or destroying.
- g) Breach Notification. In the event the Vendor becomes aware of any Security Breach due to Vendor acts or omissions other than in accordance with the terms of the Agreement, the Vendor shall, at its own expense, (1) immediately notify the State's Agreement Administrator of such Security Breach and perform a root cause analysis thereon; (2) investigate such Security Breach; (3) provide a remediation plan, acceptable to the State, to address the Security Breach and prevent any further incidents; (4) conduct a forensic investigation to determine what systems, data and information have been affected by such event; and (5) cooperate with the State, and any law enforcement or regulatory officials, credit reporting companies, and credit card associations investigating such Security Breach. The State shall make the final decision on notifying the State's persons, entities, employees, service providers and/or the public of such Security Breach, and the implementation of the remediation plan. If a notification to a customer is

required under any Law or pursuant to any of the State's privacy or security policies, then notifications to all persons and entities who are affected by the same event (as reasonably determined by the State) shall be considered legally required.

- h) Notification Related Costs. The Vendor shall reimburse the State for all Notification Related Costs incurred by the State arising out of or in connection with any such Security Breach due to Vendor acts or omissions other than in accordance with the terms of the Agreement resulting in a requirement for legally required notifications. "Notification Related Costs" shall include the State's internal and external costs associated with addressing and responding to the Security Breach including, but not limited to, (1) preparation and mailing or other transmission of legally required notifications; (2) preparation and mailing or other transmission of such other communications to customers, agents or others as the State deems reasonably appropriate; (3) establishment of a call center or other communications procedures in response to such Security Breach (e.g., customer service FAQs, talking points and training); (4) public relations and other similar crisis management services; (5) legal and accounting fees and expenses associated with the State's investigation of and response to such event; and (6) costs for credit reporting services that are associated with legally required notifications or are advisable, in the State's opinion, under the circumstances. If the Vendor becomes aware of any Security Breach which is not due to Vendor acts or omissions other than in accordance with the terms of the Agreement, the Vendor shall immediately notify the State of such Security Breach, and the parties shall reasonably cooperate regarding which of the foregoing or other activities may be appropriate under the circumstances, including any applicable Charges for the same.
- i) The Vendor shall allow the State reasonable access to Services security logs, latency statistics, and other related Services security data that affect this Agreement and the State's Data, at no cost to the State.
- j) In the course of normal operations, it may become necessary for the Vendor to copy or move Data to another storage destination on its online system, and delete the Data found in the original location. In any such event, the Vendor shall preserve and maintain the content and integrity of the Data, except by prior written notice to, and prior written approval by, the State.
- k) Remote access to Data from outside the continental United States including, without limitation, remote access to Data by authorized Services support staff in identified support centers, is prohibited unless approved in advance by the State Chief Information Officer or the Using Agency.
- l) In the event of temporary loss of access to Services, the Vendor shall promptly restore continuity of Services, restore Data in accordance with this Agreement and as may be set forth in an SLA, restore accessibility of Data and the Services to meet the performance requirements stated herein or in an SLA. As a result, Service Level remedies will become available to the State as provided herein, in the SLA or other agreed and relevant documents. Failure to promptly remedy any such temporary loss of access may result in the State exercising its options for assessing damages under this Agreement.
- m) In the event of disaster or catastrophic failure that results in significant State Data loss or extended loss of access to Data or Services, the Vendor shall notify the State by the fastest means available and in writing, with additional notification provided to the State Chief Information Officer or designee of the contracting agency. Vendor shall provide such notification within twenty-four (24) hours after Vendor reasonably believes there has been such a disaster or catastrophic failure. In the notification, Vendor shall inform the State of:
 - (1) The scale and quantity of the State Data loss;
 - (2) What Vendor has done or will do to recover the State Data from backups and mitigate any deleterious effect of the State Data and Services loss; and
 - (3) What corrective action Vendor has taken or will take to prevent future State Data and Services loss.
 - (4) If Vendor fails to respond immediately and remedy the failure, the State may exercise its options for assessing damages or other remedies under this Agreement.

The Vendor shall investigate the disaster or catastrophic failure and shall share the report of the investigation with the State. The State and/or its authorized agents shall have the right to lead (if required by law) or participate in the investigation. The Vendor shall cooperate fully with the State, its agents and law enforcement.

- n) In the event of termination of this contract, cessation of business by the Vendor or other event preventing the Vendor from continuing to provide the Services, the Vendor shall not withhold the State Data or any other State confidential information or refuse, for any reason, to promptly return to the State the State Data and any other State confidential information (including copies thereof) if requested to do so on such media as reasonably requested by the State, even if the State is then or is alleged to be in breach of the Agreement. As a part of the Vendor's obligation to provide the State Data pursuant to this Paragraph 18) n), the Vendor will also provide the State any data maps, documentation, software, or other materials necessary, including, without limitation, handwritten notes, materials, working papers or documentation, for the State to use, translate, interpret, extract and convert the State Data.
- o) Secure Data Disposal. When requested by the State, the Vendor shall destroy all requested data in all of its forms (e.g., disk, CD/DVD, backup tape, and paper). Data shall be permanently deleted and shall not be recoverable, in accordance with National Institute of Standards and Technology (NIST) approved methods, and certificates of destruction shall be provided to the State.

Section 3: Terms and Conditions Applicable to Information Technology Goods and Services

- 1) **SOFTWARE LICENSE FOR HARDWARE, EMBEDDED SOFTWARE AND FIRMWARE:** Reserved.
- 2) **LICENSE GRANT FOR APPLICATION SOFTWARE, (COTS):** This paragraph recites the scope of license granted, if not superseded by a mutually agreed and separate licensing agreement, as follows:
 - a) Vendor grants to the State, its Agencies and lawful customers a non-exclusive, non-transferable and non-sublicensable license to use, in object code format, Vendor's software identified in the solicitation documents, Vendor's Statement of Work (SOW), or an Exhibit thereto executed by the parties ("Software"), subject to the restrictions set forth therein, such as the authorized computer system, the data source type(s), the number of target instance(s) and the installation site. Use of the Software shall be limited to the data processing and computing needs of the State, its Agencies and lawful customers. This license shall be perpetual or for the term of the contract (pick one, delete the other), unless terminated as provided herein. The State agrees not to distribute, sell, sublicense or otherwise transfer copies of the Software or any portion thereof. For purposes of this Agreement, a State Entity shall be defined as any department or agency of the State of North Carolina, which is controlled by or under common control of the State or who is a lawful customer of the State pursuant to Article 3D of Chapter 147 of the General Statutes.
 - b) Vendor shall provide all encryption or identification codes or authorizations that are necessary or proper for the operation of the licensed Software.
 - c) The State shall have the right to copy the Software, in whole or in part, for use in conducting benchmark or acceptance tests, for business recovery and disaster recovery testing or operations, for archival or emergency purposes, for back up purposes, for use in preparing derivative works if allowed by the solicitation documents or statements of work, or to replace a worn copy.
 - d) The State may modify non-personal Software in machine-readable form for its internal use in merging the same with other software program material. Any action hereunder shall be subject to uses described in this paragraph, the restrictions imposed by Paragraph 3), and applicable terms in the solicitation documents or statements of work.
- 3) **WARRANTY TERMS:** Notwithstanding anything in the Agreement or Exhibit hereto to the contrary, Vendor shall assign warranties for any Deliverable supplied by a third party to the State.
 - a) a) Vendor warrants that any Software or Deliverable will operate substantially in conformity with prevailing specifications as defined by the current standard documentation (except for minor defects or errors which are not material to the State) for a period of ninety (90) days from the date of acceptance ("Warranty Period"), unless otherwise specified in the Solicitation Documents. If the Software does not perform in accordance with such specifications during the Warranty Period, Vendor will use reasonable efforts to correct any deficiencies in the Software so that it will perform in accordance with or substantially in accordance with such specifications.

- b) Vendor warrants to the best of its knowledge that:
 - i) The licensed Software and associated materials do not infringe any intellectual property rights of any third party;
 - ii) There are no actual or threatened actions arising from, or alleged under, any intellectual property rights of any third party;
 - iii) The licensed Software and associated materials do not contain any surreptitious programming codes, viruses, Trojan Horses, "back doors" or other means to facilitate or allow unauthorized access to the State's information systems.
 - iv) The licensed Software and associated materials do not contain any timer, counter, lock or similar device (other than security features specifically approved by Customer in the Specifications) that inhibits or in any way limits the Software's ability to operate.
- c) UNLESS MODIFIED BY AMENDMENT OR THE SOLICITATION DOCUMENTS, THE WARRANTIES IN THIS PARAGRAPH ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, OR WHETHER ARISING BY COURSE OF DEALING OR PERFORMANCE, CUSTOM, USAGE IN THE TRADE OR PROFESSION OR OTHERWISE, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, AND NO OTHER REPRESENTATIONS OR WARRANTIES HAVE FORMED THE BASIS OF THE BARGAIN HEREUNDER.

4) RESTRICTIONS: State's use of the Software is restricted as follows:

- a) The license granted herein is granted to the State and to any political subdivision or other entity permitted or authorized to procure Information Technology through the Department of Information Technology. If the License Grant and License Fees are based upon the number of Users, the number of Users may be increased at any time, subject to the restrictions on the maximum number of Users specified in the solicitation documents.
- b) No right is granted hereunder to use the Software to perform Services for commercial third parties (so-called "service bureau" uses). Services provided to other State Departments, Agencies or political subdivisions of the State is permitted.
- c) The State may not copy, distribute, reproduce, use, lease, rent or allow access to the Software except as explicitly permitted under this Agreement, and State will not modify, adapt, translate, prepare derivative works (unless allowed by the solicitation documents or statements of work,) decompile, reverse engineer, disassemble or otherwise attempt to derive source code from the Software or any internal data files generated by the Software.
- d) State shall not remove, obscure or alter Vendor's copyright notice, trademarks, or other proprietary rights notices affixed to or contained within the Software.

5) SUPPORT OR MAINTENANCE SERVICES: This paragraph recites the scope of maintenance Services due under the license granted, if not superseded by a separate licensing and maintenance agreement or as may be stated in the solicitation documents. Subject to payment of a Support Service or Maintenance Fee stated in the solicitation documents for the first year and all subsequent years, if requested by the State, Vendor agrees to provide the following support Services ("Support Services") for the current version and one previous version of the Software commencing upon delivery of the Software:

- a) **Error Correction:** If the error conditions reported by the State pursuant to the General Terms and Conditions are not corrected in a timely manner, the State may request a replacement copy of the licensed Software from Vendor. In such event, Vendor shall then deliver a replacement copy, together with corrections and updates, of the licensed Software within 24 hours of the State's request at no added expense to the State.
- b) **Other Agreement:** This Paragraph 5 may be superseded by written mutual agreement provided that: Support and maintenance Services shall be fully described in such a separate agreement annexed hereto and incorporated herein
- c) **Temporary Extension of License:** If any licensed Software or CPU/computing system on which the Software is installed fails to operate or malfunctions, the term of the license granted shall be temporarily extended to another CPU selected by the State and continue until the earlier of:
 - i) Return of the inoperative CPU to full operation, or

- ii) Termination of the license.
 - d) **Encryption Code:** Vendor shall provide any temporary encryption code or authorization necessary or proper for operation of the licensed Software under the foregoing temporary license. The State will provide notice by expedient means, whether by telephone, e-mail or facsimile of any failure under this paragraph. On receipt of such notice, Vendor shall issue any temporary encryption code or authorization to the State within twenty-four (24) hours; unless otherwise agreed.
 - e) **Updates:** Vendor shall provide to the State, at no additional charge, all new releases and bug fixes (collectively referred to as "Updates") for any Software Deliverable developed or published by Vendor and made generally available to its other customers at no additional charge. All such Updates shall be a part of the Program and Documentation and, as such, be governed by the provisions of the Agreement.
 - f) **Telephone Assistance:** Vendor shall provide the State with telephone access to technical support engineers for assistance in the proper installation and use of the Software, and to report and resolve Software problems, during normal business hours, 8:00 AM - 5:00 PM Eastern Time, Monday-Friday. Vendor shall respond to the telephone requests for Program maintenance service, within four (4) hours or eight (8) hours or next business day, etc. *(edit this time to what you want your response time to be)*, for calls made at any time
- 6) **STATE PROPERTY AND INTANGIBLES RIGHTS:** The parties acknowledge and agree that the State shall own all right, title and interest in and to the copyright in any and all software, technical information, specifications, drawings, records, documentation, data and other work products first originated and prepared by the Vendor for delivery to the State (the "Deliverables"). To the extent that any Vendor Technology is contained in any of the Deliverables, the Vendor hereby grants the State a royalty-free, fully paid, worldwide, perpetual, non-exclusive license to use such Vendor Technology in connection with the Deliverables for the State's internal business purposes. Vendor shall not acquire any right, title and interest in and to the copyrights for goods, any and all software, technical information, specifications, drawings, records, documentation, data or derivative works thereof, or other work products provided by the State to Vendor. The State hereby grants Vendor a royalty-free, fully paid, worldwide, perpetual, non-exclusive license to non-confidential Deliverables first originated and prepared by the Vendor for delivery to the State.

Section 4: Terms and Conditions Applicable to Personnel and Personal Services

- 1) **VENDOR'S REPRESENTATION:** Vendor warrants that qualified personnel will provide Services in a professional manner. "Professional manner" means that the personnel performing the Services will possess the skill and competence consistent with the prevailing business standards in the information technology industry. Vendor agrees that it will not enter any agreement with a third party that might abridge any rights of the State under the Agreement. Vendor will serve as the prime Vendor under the Agreement. Should the State approve any subcontractor(s), the Vendor shall be legally responsible for the performance and payment of the subcontractor(s). Names of any third-party Vendors or subcontractors of Vendor may appear for purposes of convenience in Contract documents; and shall not limit Vendor's obligations hereunder. Such third-party subcontractors, if approved, may serve as subcontractors to Vendor. Vendor will retain executive representation for functional and technical expertise as needed in order to incorporate any work by third party subcontractor(s).

- a) Intellectual Property. Vendor represents that it has the right to provide the Services and other Deliverables without violating or infringing any law, rule, regulation, copyright, patent, trade secret or other proprietary right of any third party. Vendor also represents that its Services and other Deliverables are not the subject of any actual or threatened actions arising from, or alleged under, any intellectual property rights of any third party.
 - b) Inherent Services. If any Services or other Deliverables, functions, or responsibilities not specifically described in the Agreement are required for Vendor's proper performance, provision and delivery of the Services and other Deliverables pursuant to the Agreement, or are an inherent part of or necessary sub-task included within the Services, they will be deemed to be implied by and included within the scope of the Contract to the same extent and in the same manner as if specifically described in the Contract.
 - c) Vendor warrants that it has the financial capacity to perform and to continue to perform its obligations under the Contract; that Vendor has no constructive or actual knowledge of an actual or potential legal proceeding being brought against Vendor that could materially adversely affect performance of the Agreement; and that entering into the Agreement is not prohibited by any Contract, or order by any court of competent jurisdiction.
- 2) **SERVICES PROVIDED BY VENDOR:** Vendor shall provide the State with implementation Services as specified in a Statement of Work ("SOW") executed by the parties. This Agreement in combination with each SOW individually comprises a separate and independent contractual obligation from any other SOW. A breach by Vendor under one SOW will not be considered a breach under any other SOW. The Services intended hereunder are related to the State's implementation and/or use of one or more Software Deliverables licensed hereunder or in a separate software license agreement between the parties ("License Agreement"). (Reserve if not needed)
- 3) **PERSONNEL:** Vendor shall not substitute key personnel assigned to the performance of the Agreement without prior written approval by the Agency Contract Administrator. The individuals designated as key personnel for purposes of the Agreement are those specified in the Vendor's offer. Any desired substitution shall be noticed to the Agency's Contract Administrator in writing accompanied by the names and references of Vendor's recommended substitute personnel. The Agency will approve or disapprove the requested substitution in a timely manner. The Agency may, in its sole discretion, terminate the Services of any person providing Services under the Agreement. Upon such termination, the Agency may request acceptable substitute personnel or terminate the Contract Services provided by such personnel.
- a) Unless otherwise expressly provided in the Contract, Vendor will furnish all of its own necessary management, supervision, labor, facilities, furniture, computer and telecommunications equipment, software, supplies and materials necessary for the Vendor to provide and deliver the Services and other Deliverables.
 - b) Vendor personnel shall perform their duties on the premises of the State, during the State's regular workdays and normal work hours, except as may be specifically agreed otherwise, established in the specification, or statement of work.
 - c) The Agreement shall not prevent Vendor or any of its personnel supplied under the Agreement from performing similar Services elsewhere or restrict Vendor from using the personnel provided to the State, provided that:
 - i) Such use does not conflict with the terms, specifications or any amendments to the Agreement, or
 - ii) Such use does not conflict with any procurement law, regulation or policy, or
 - iii) Such use does not conflict with any non-disclosure agreement, or term thereof, by and between the State and Vendor or Vendor's personnel.
 - d) Unless otherwise provided by the Agency, the Vendor shall furnish all necessary personnel, Services, and otherwise perform all acts, duties and responsibilities necessary or incidental to the accomplishment of the tasks specified in the Agreement. The Vendor shall be legally and financially responsible for its personnel including, but not limited to, any deductions for social security and other withholding taxes required by state or federal law. The Vendor shall be solely responsible for

acquiring any equipment, furniture, and office space not furnished by the State necessary for the Vendor to comply with the Agreement. The Vendor personnel shall comply with any applicable State facilities or other security rules and regulations.

- 4) **PERSONAL SERVICES:** The State shall have and retain the right to obtain personal Services of any individuals providing Services under the Agreement. This right may be exercised at the State's discretion in the event of any transfer of the person providing personal Services, termination, default, merger, acquisition, bankruptcy or receivership of the Vendor to ensure continuity of Services provided under the Agreement. Provided, however, that the Agency shall not retain or solicit any Vendor employee for purposes other than completion of personal Services due as all or part of any performance due under the Agreement.
- a) Vendor personnel shall perform any duties on the premises of the State during the State's regular workdays and normal work hours, except as may be specifically agreed otherwise, established in the specification, or statement of work.
 - b) The State has and reserves the right to disapprove the continuing assignment of Vendor personnel provided by Vendor under the Agreement. If this right is exercised and the Vendor is not able to replace the disapproved personnel as required by the State, the parties agree to employ best commercial efforts to informally resolve such failure equitably by adjustment of other duties, set-off, or modification to other terms that may be affected by Vendor's failure.
 - c) Vendor will make every reasonable effort consistent with prevailing business practices to honor the specific requests of the State regarding assignment of Vendor's employees. Vendor reserves the sole right to determine the assignment of its employees. If one of Vendor's employees is unable to perform due to illness, resignation, or other factors beyond Vendor's control, Vendor will provide suitable personnel at no additional cost to the State.
 - d) The Agreement shall not prevent Vendor or any of its personnel supplied under the Agreement from performing similar Services elsewhere or restrict Vendor from using the personnel provided to the State, provided that:
 - i) Such use does not conflict with the terms, specifications or any amendments to the Agreement, or
 - ii) Such use does not conflict with any procurement law, regulation or policy, or
 - iii) Such use does not conflict with any non-disclosure agreement, or term thereof, by and between the State and Vendor or Vendor's personnel.

ATTACHMENT C: DEPARTMENT OF HEALTH AND HUMAN SERVICES TERMS AND CONDITIONS

C.1 NCDHHS PRIVACY AND SECURITY OFFICE (PSO) TERMS

C.1.1 COMPLIANCE WITH APPLICABLE LAWS

The Vendor shall comply with all electronic storage standards concerning privacy, data protection, confidentiality, and security including those of federal, state, and DHHS having jurisdiction where business services are provided for accessing, receiving, or processing all confidential information.

STATE AND NC DEPARTMENT OF HEALTH AND HUMAN SERVICES PRIVACY AND

The Vendor shall implement internal data security measures, and other industry security best practices utilizing appropriate hardware and software necessary to monitor, maintain, and ensure data integrity in accordance with all applicable federal regulations, state regulations, DHHS privacy and security policies. The Vendor will maintain all Privacy and security safeguards throughout the term of this agreement. In addition, the Vendor agrees to maintain compliance with the following:

- a) NC DHHS Privacy Manual and Security Manual, both located online at:

<https://policies.ncdhhs.gov/departamental/policies-manuals/section-viii-privacy-and-security>

C.1.2 HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)

If the DHHS Division or Office determines that some or all the activities within the scope of this contract are subject to the Health Insurance Portability and Accountability Act of 1996, P.L. 104-91, as amended (HIPAA), or its implementing regulations, the Vendor agrees to comply with all HIPAA requirements and will execute such agreements and practices as the Division or Office may require ensuring compliance.

C.1.3 CONFIDENTIALITY

- a) The Vendor shall adhere to DHHS privacy and security policies, as well as those in the federal regulations including Rule at 45 C.F.R. Parts 160 and 164, subparts A and E , Security Standards at 45 C.F.R. Parts 160, 162 and 164, subparts A and C (“the Security Rule”), and the applicable provisions of the Health Information Technology for Economic and Clinical Health Act (HITECH).
- b) **DUTY TO REPORT:** In addition to any DHHS Privacy and Security Office (PSO) notification requirements in a Business Associate Agreement (BAA) with a DHHS Division or Office pr om the North Carolina Department of Information Technology Terms and Conditions, the Vendor shall (1) report all suspected and confirmed privacy/security incidents or privacy/security breaches involving unauthorized access, use, disclosure, modification, or data destruction to the DHHS Privacy and Security Office at <https://www.ncdhhs.gov/about/administrative-divisions-offices/office-privacy-security> within twenty-four (24) hours after the incident is first discovered. (2) If the privacy or security incident involves Social Security Administration (SSA) data or Centers for Medicare and Medicaid Services (CMS) data, the vendor shall report the incident within

one (1) hour after the incident is first discovered. At a minimum, such privacy and security incident report will contain to the extent known: the nature of the incident, specific information about the data compromised, the date the privacy or security incident occurred, the date the Vendor was notified, and the identity of affected or potentially affected individual(s). (3) During the performance of this contract, the vendor is to notify the DHHS Privacy and Security Office of any contact by the federal Office for Civil Rights (OCR) received by the vendor. In addition, the Vendor will reasonably cooperate with DHHS Divisions and Offices to mitigate the damage or harm of such security incidents.

C.1.4 CONTINUOUS MONITORING

- a) The Vendor shall maintain compliance with the State Chief Information Officer's (CIO) Continuous Monitoring Process mandate, requiring that Vendors hosting state-owned data outside of NC DIT's infrastructure environment work with state agencies to implement a risk management program that continuously monitors risk through the performance of assessments, risk analysis, and data inventory.
- b) Based upon NIST 800-137, "Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations", the Vendor shall perform security/risk assessments on its information systems using the latest NIST 800-53 controls to assess its compliance with enterprise security standards as outlined below.

Security Assessment:

- i. Vendors providing Infrastructure as a Service, Platform as a Service and/or Software as a Service for the state agency are required to obtain approval from the DHHS Privacy and Security Office to ensure their compliance with statewide security policies.
- ii. To obtain such approval, the Vendor shall annually provide both a written attestation to its compliance and an industry recognized, third party assessment report, such as the Federal Risk and Authorization Management Program (FedRAMP) certification, SOC 2 Type 2, HITRUST CSF and ISO 27001. State agencies will be required to review these security assessment reports, assess the risk of each vendor, ensure completion of all findings using a Corrective Action Plan (CAP), and provide an annual certification to the Vendor's compliance to the State CIO.

The Vendor shall work with the state agency to provide a data inventory of all cloud hosted services, by assisting the state agency with completing a Privacy Threshold Analysis (PTA) documenting the data classification and the data fields hosted within the cloud, offsite, or Vendor-hosted environment. The Vendor shall review a Privacy Threshold Analysis (PTA) with the NC DHHS Privacy and Security Office annually and assist with updating the PTA when changes to the data being hosted occur.

DHHS Privacy & Security office may perform periodic independent security assessments of Vendor hosted applications on the public/private/hybrid cloud or On-Prem data centers. The Vendor must provide access to their applications' hosting environment and their key resources to DHHS designated resources and DHHS engaged vendors to perform a privacy & security risk assessment that includes vulnerability analysis, penetration testing,

and risk analysis based on the latest NIST 800-53, Federal, State and DHHS requirements.

C.1.5 OVERSIGHT

- a) **RECORD RETENTION:** Records shall not be destroyed, purged, or disposed of without the express written consent of the DHHS Division or Office. State basic records retention policy requires all grant records to be retained for a minimum of five years or until all audit exceptions have been resolved, whichever is longer. If the contract is subject to federal policy and regulations, record retention may be longer than five years. Records must be retained for a period of three years following submission of the final Federal Financial Status Report, if applicable, or three years following the submission of a revised final Federal Financial Status Report. Also, if any litigation, claim, negotiation, audit, disallowance action, or other action involving this Contract has been started before expiration of the five-year retention period described above, the records must be retained until completion of the action and resolution of all issues which arise from it, or until the end of the regular five-year period described above, whichever is later. The record retention period for Temporary Assistance for Needy Families (TANF) and MEDICAID and Medical Assistance grants and programs is a minimum of ten years. The record retention period for the Health Insurance Portability and Accountability Act (HIPAA) is six years. For the Internal Revenue Service (IRS) and the Social Security Administration (SSA), the record retention period is seven years.

C.1.6 FLOW-DOWN

In addition to the subcontracting requirements in Paragraph 4) of the NCDIT Terms and Conditions, Attachment B, Section 1: (1) if a sub-contractor is used in the performance of this contract, written approval of the NC DHHS PSO (Privacy and Security Office) is also required; and (2) Vendor must include without modification all the security and privacy terms and conditions in this Attachment C, Department of Health and Human Services Terms and Conditions in each sub-contract.

C.2 TRANSITION ASSISTANCE

If the Contract is not renewed at the end of this term, or is canceled prior to its expiration, for any reason, the Vendor must provide for up to three (3) months after the expiration or cancellation of the Contract ("Transition Period"), all reasonable transition assistance requested by the Agency, to allow for the expired or canceled portion of the Services to continue without interruption or adverse effect, and to facilitate the orderly transfer of such Services to the Agency or its designees. Such transition assistance will be deemed by the parties to be governed by the terms and conditions of the Contract, (notwithstanding this expiration or cancellation) except for those Contract terms or conditions that do not reasonably apply to such transition assistance. The Agency shall pay the Vendor for any resources utilized in performing such transition assistance at the most current rates provided by the Agreement for Contract performance. If the State cancels the Agreement for cause, then the Agency will be entitled to offset the cost of paying the Vendor for the additional resources the Vendor utilized in providing transition assistance with any damages the Agency may have otherwise accrued as a result of said cancellation.

- a. In the event transition assistance becomes necessary, the Parties will meet to discuss transition, including turnover procedures, the transition meeting schedule, and any risks, barriers, assumptions, and mitigation strategies for transition.
- b. During the Transition Period, the Vendor will continue to provide services to the Agency without cessation or alteration. The Transition Period may be modified as agreed upon in writing by the parties in a Contract amendment, including adding additional transition services.
- c. The Vendor will provide a draft of its Transition Plan to the Agency within ninety (90) calendar days after Contract award. The Transition Plan will describe how the Vendor will transition responsibility to the Agency or its designees if a Transition Event occurs. The Transition Plan must adhere to the requirements included in Attachment J. MINIMUM CONTENT FOR PROJECT AND O&M DELIVERABLES.
- d. Within thirty (30) calendar days of receiving/providing notice of intent to terminate or of Contract expiration and no later than ninety (90) calendar days prior to termination or expiration of the Contract, the Vendor will develop and deliver to the Agency an updated Transition Plan. The updated Transition Plan will document the steps required to transition the Confidential Information from the Vendor to the Agency or its designee. The Vendor will obtain the Agency's approval of its updated Transition Plan and will be required to update and obtain the Agency's approval of revisions to its plan as revisions are made.
- e. If the Solution is Vendor-Hosted, the Vendor will be required to perform both the tasks included above in paragraphs 12) a)-d) and the additional tasks listed below:
 - i. During the Transition Period, the Vendor will extract and/or transition to the Agency a full backup of all Agency's Confidential Information/State Data collected, stored, and maintained by the Solution in an agreed upon usable format, at no cost to the Agency. The Agency's Confidential Information/State Data will be delivered to the Agency no later than sixty (60) calendar days after the start of the Transition Period, at no cost to the Agency. At the request of the Agency, the Vendor will be required to provide technical support for at least thirty (30) calendar days after delivering the Agency's Confidential Information/State Data to the Agency for the purpose of assuring the format and contents of the Agency's Confidential Information/State Data are accurate and meet the needs of the Agency. The Agency's Confidential Information/State Data must be organized by Entity Relationship Diagram (ERD) and accompanied by the following documentation unless this documentation is being maintained by State technical staff:
 1. Diagram of all the Solution tables and databases;
 2. Data dictionaries for all tables/databases; and
 3. Related reference files and coding guides.
 - ii. Upon receiving written notice from the Agency, the Vendor will destroy or purge any Confidential Information provided by or for the Agency during the Contract term, from all Vendor or hosting service provider databases, electronic files, or paper files (including backups). This destruction or purge should only occur following both the Vendor's receipt of the Agency's written request and the Agency's confirmation that the Agency's Confidential Information/State Data has been delivered and received in a usable,

archivable format. When the Agency directs the Vendor to destroy or purge all Confidential Information/State Data within its and its hosting service provider's infrastructure and possession, in electronic or paper form, the Vendor and the hosting service provider will be required to certify in writing within thirty (30) calendar days of the Vendor receiving such written notice that all Confidential Information/State Data referenced above has been destroyed or purged.

- iii. The Vendor will be required to ensure that its hosting service provider, if any, also complies with the Transition Period obligations in this section.
- iv. Until the Vendor has certified the completion of the data destruction or purge, the Vendor will continue to comply with all data security sections within this RFP even after the resulting Contract has terminated or expired.

C. 3Stablization

During the Project Execution Phase, Vendor will provide support until the Solution has been stabilized. The Solution will be deemed "stable" when it is available and has been operating continuously for ninety (90) consecutive Calendar Days following Deployment so that users can successfully log into the Solution and perform their daily work 24x7x365 (excluding scheduled maintenance periods) without frequent system lockups, freezes, or shutdowns. If a Category 1, 2 or 3 Defect or issue occurs during the 90-day Stabilization Period, the Vendor must resolve the Defect/issue in accordance with the table below and the Defect/issue must remain resolved by the end of the 90-day Stabilization Period or resolved within the Defect resolution time outlined below for Defects that occur at the end of the Stabilization Period and the resolution time extends beyond the 90-day Stabilization Period. Any Defect that is not resolved within the specified timeframe is subject to the Liquidated damages outlined below. These Severity 1, 2, or 3 Defects do not include any issues that may arise that are outside of Vendor responsibility, which are also summarized below. The Severity Levels are defined in the following table and will be included in the Service Level Agreement.

Liquidated Damages. The State and the Vendor agree to the specific standards set forth in this Contract. Vendor shall maintain and follow the Service Level Agreement below. It is agreed between the Vendor and the State that the failure to meet the Service/Performance Levels identified in the Service Level Agreement below would cause damages to the State that would be difficult or impossible to determine with accuracy. The Vendor agrees that its failure to meet the Service/Performance Level may or will affect the delivery of (goods/services, etc.), either directly or indirectly and may or will result, directly or proximately, in monetary damages to the State; therefore, the actual amount of such injury and damage will be impossible or extremely difficult to calculate. The State and the Vendor therefore agree that the liquidated damages set out in the table below shall be a reasonable approximation of the damages that shall be suffered by the State.

- 1) Vendor agrees that the Vendor shall pay liquidated damages to the State in the instances and in the amounts set forth in the below table. The Parties also agree that the stated liquidated damage amounts are reasonable and not punitive. Accordingly, in the event of such damages, at the written direction of the State, the Vendor shall pay the State the indicated amount as liquidated damages, and not as a penalty.
- 2) Amounts due the State as liquidated damages, if not paid by the Vendor within fifteen (15) days of notification of assessment, may be deducted by the State from any money payable to the Vendor pursuant to this Contract. The State will notify the Vendor in writing of any claim for liquidated damages pursuant to this paragraph on or before the date the State deducts such sums from money payable to the Vendor. No delay by the State in assessing or collecting liquidated

damages shall be construed as a waiver of such rights. The imposition and payment of liquidated damages shall not affect or waive any other rights of the State to enforce or terminate this Contract. In cases where actual damages can be determined, liquidated damages shall not apply.

3) If the State elects not to impose liquidated damages in a particular instance, this decision shall not be construed as a waiver of the State's right to pursue future assessment of performance standards and associated liquidated damages; nor construed to limit any additional remedies available to the State.

4) The Vendor shall not be liable for liquidated damages when, in the opinion of the State, incidents or delays result directly from causes beyond the control and without the fault or negligence of the Vendor. Such causes may include, but are not restricted to, acts of God, fires, floods, epidemics, labor unrest, and third-party carrier matters outside the control of Vendor; but in every case the delays must be beyond the control and without the fault or negligence of the Vendor.

The Service performance Levels and liquidated damage for each are as follows:

Category	Description	Response Time	Diagnosis Time	Resolution Time	Remedy
Category 1 (Major Problem)	An outage that results in the unavailability of the Solution or the Solution's hosting environment or a Defect that has persisted at the Severity 2 level for more than 48 hours.	1 hour	1 hour	24 hours	1. \$100 per minute beyond the resolution time
Category 2 (Critical Problem)	An outage where the Solution or the Solution's hosting environment is available but one or more of the Critical Functions provided by the Solution is not operational, and a Workaround does not exist, or a Severity 3 problem that has persisted for more than five (5) business days.	1-2 hours	24 hours	48 hours	1. \$75 per minute beyond the resolution time
Category 3 (Minor Problem)	Degradation of Non-Critical System Functions that has persisted for more than eight (8)	1 business day	3 business days	5 business days	1. \$35 per minute beyond the resolution time

Category	Description	Response Time	Diagnosis Time	Resolution Time	Remedy
	business hours.				
Category 4 (Changes)	Request for Changes to the Solution.	3 business days	5 business days	N/A	N/A
Category 5 (General Requests)	General questions or informal contacts.	3 business days	5 business days	2 business weeks	N/A



Solicitation Addendum

Solicitation Number: 30-23189

Solicitation Description: DCDEE – Workforce Registry and NC Pre-K and Regulatory System Replacement

Solicitation Opening Date and Time: August 14, 2023
2:00 PM EST

Addendum Number: 1

Addendum Date: July 21, 2023

Contract Specialist or Purchasing Agent: *Jillian Kennedy, Contract Specialist*
Jillian.kennedy@dhhs.nc.gov

1. Vendor must return one properly executed copy of this addendum with bid response or prior to the Bid Opening Date/Time listed above.

2. The solicitation is hereby modified as follows:

a) Section **2.2 CONTRACT TERM** on page 5 shall be replaced with the following:

A contract awarded pursuant to this RFP shall have an effective date as provided in the Notice of Award. The term shall be **three (3) year(s)** and will expire upon the anniversary date of the effective date unless otherwise stated in the Notice of Award, or unless terminated earlier. The State retains the option to extend the Agreement for **two (2) one(1) year** renewal period at its sole discretion.

b) Section **5.2 EVALUATION CRITERIA** on page 27 shall be replaced with the following:

5.2 EVALUATION CRITERIA

Evaluation shall include best value, as the term is defined in N.C.G.S. § 143-135.9(a)(1), compliance with information technology project management policies as defined by N.C.G.S. §143B-1340, compliance with information technology security standards and policies, substantial conformity with the specifications, and other conditions set forth in the solicitation. The following Evaluation Criteria are listed in Order of Importance.

1. Substantial conformity to the specifications (Section 3.0)

2. Technical Approach (Section 3.0)

3. Past Performance and Experience (includes the following) (Section 6.3)

a. Experience of similar size, scope, complexity, and magnitude of effort to that of the solicitation

b. References

4. Financial Viability (Section 7.0)
5. Total Cost of Ownership (Section 7.0)

c) Specifications for Integration and System Interfaces on page 147 shall be replaced with the following:

Integration and System Interfaces	INI_1	DIT- Describe the solutions ability to Integrate with the State agencies authentication platforms.
	INI_3	DPI- Describe the solutions ability to receive file/real time information about Licensed teachers & send information on enrollee's (teacher's) training from Department of Public Instruction Online Licensure System. Describe the solutions ability to receive wage and Licensure file; send new approved lead NC Pre-k teacher from Department of Public Instruction Human Resource Management System.
	INI_4	Describe the solutions ability to receive file containing the names of adults flagged for maltreatment from the Child Maltreatment Registry.
	INI_5	Describe how the solution shares facility and workforce qualification data between workforce and regulatory areas and keeps information current.
	INI_6	Describe the solutions ability to integrate or receive data from Training platforms such as Moodle, Voyage Sporis & Teaching Strategies for enrollees.
	INF_7	Describe the solutions ability to integrate with partnership agencies application to receive and provide information to end users. CCSA-Receive a list of bonus approval administered. CCSA Grants System – (T.E.A.C.H., WAGES, AWARD Plus and AWARDS) Receive files with enrollee grant and wage information.
	INI_8	North Carolina Institute for CDP – Send a list of EEC certifications granted.
	INI_9	Describe the solution ability to integrate with external agencies to receive Health and Safety trainers' information
	INF_10	CBC/ABCMS-Real time integration with CBC for background check of enrollees
	INI_11	Describe the ability of the solution to Integrate with state approved payment platforms for training payments

	INI_12	Describe the solutions ability to Integrate or receive monthly file from Vital Records application
	INI_13	Describe the solutions ability to integrate with Clearing houses to receive Official Transcripts.
	INI_14	Describe the solutions ability to integrate with NCRLAP to view, assign, or participate in trainings
	INI_15	Describe the solutions ability to integrate with NC Pre-K's application to route change requests for appropriate approvals by EES and Workforce Education Unit.
	INI_16	Describe the solutions ability to integrate with Scribbles to add, retrieve, annotate, and manage documents.

3. Following are questions received about the solicitation and the State's answers to the questions.

Question #	Solicitation Section	Solicitation Subsection	Vendor Question	Agency Response
1	2.2 Contract Term Attachment E: Cost Form	a) Cost Table 2: Operations and Maintenance	Please clarify the contract terms for submission of pricing for the initial term and optional years.	Please see above change to the solicitation.
2	3.5 Management Specifications	3.5.5 Data Conversion and Migration	Are there any systems other than Regulatory, WORKS, and NC Pre-K in scope for data migration?	No.
3	3.5 Management Specifications	3.5.5 Data Conversion and Migration	What data should be migrated from the existing systems? Is the scope limited to a subset of the data or all data in the systems? How many tables and records comprise each existing/legacy system?	WORKS: All Data should be migrated. 40 tables and 192,209 records. NC Pre-K: All Data should be migrated. 198 tables and 27,394 records. Regulatory: All Data. Approximately 20+ tables and 5,414,554 records.
4	3.5 Management Specifications	3.5.5 Data Conversion and Migration	Please provide the database structure of NC Pre-K (ex: Oracle, MySQL, etc.).	Oracle DB. The NC Pre-K database has data for Children, Sites, Classrooms, Teacher's Licensure and Education, Contracting Agencies and Budget.

Question #	Solicitation Section	Solicitation Subsection	Vendor Question	Agency Response
5	3.5 Management Specifications	3.5.6 Operations and Maintenance 6.0 Help Desk Support	Is the expectation that the Vendor Help Desk would provide system support to all user types, including external users such as outlined in Attachment L, Workforce Registration REG 1 (Mentors & Evaluators, Teachers (both Lead and Assistants), Technical Assistance Providers, Early childhood and school age administrators, Students training in early education, Program Coordinator, Prospective Childcare owners and Facility Owners/Directors, and Prospective Teachers), or would external users contact the Agency Help Desk for their system support inquiries?	Workforce Registry: Yes. Also, engage with DHHS and NCDIT for issues related to State's systems. NC Pre-K: Yes. Also, engage with DHHS and NCDIT for issues related to State's systems. Regulatory: Yes. Also, engage with DHHS and NCDIT for issues related to State's systems. EES: Ensure the business-related questions are routed to the EES team.
6	Attachment L:	REG_1	Please confirm the number of expected users by type as included in REG_1, Attachment L: 1. Mentors & Evaluators 2. Teachers (both Lead and Assistants) 3. Technical Assistance Providers 4. Early childhood and school age administrators 5. Students training in early education 6. Program Coordinator 7. Prospective Childcare owners and Facility Owners/Directors 8. Prospective Teachers	1. Mentors & Evaluators: 60 2. Teachers (both Lead and Assistants): Lead Teacher only in public and private school-2000. 7. Prospective Childcare owners and Facility Owners/Directors: We currently have 5450 childcare facilities (centers-4354 and homes - 1196). Some facilities may have more than one owner and some owners may own more than one facility. Therefore, the number of owners will not match the number of facilities. We do not collect other information and can't provide that data.
7			What is the budget for this project?	In accordance with 09 NCAC 06B .0103 – Confidentiality of Solicitation Documents: In order to preserve fairness and encourage competitiveness, all information and documentation relative to the development of a solicitation for a proposed procurement shall be withheld from public inspection. Refer to cited rule above for complete language.

Question #	Solicitation Section	Solicitation Subsection	Vendor Question	Agency Response
8			Is there a planned payment schedule based on project phases?	The Vendor shall propose its itemized payment schedule based on the content of its offer. All payments must be based upon acceptance of one or more Deliverables during Project Execution Contract Phase.
9	ATTACHMENT L: WORKFORCE REGISTRY	WF_6-9, WF_11 – Page 144, 145 INI_6 – Page 147	Does DHHS intend to use an existing LMS platform for integration with the Workforce Registry, or should the vendor propose a LMS solution for training/coursework assignment? If using an existing LMS platform, please confirm Moodle, Voyage Sporis and Teaching Strategies are the only integrations.	Yes. Currently, Programs use Moodle. Proposals can include other LMS platforms, but they need to meet Business needs for a LMS including data reporting.
10	ATTACHMENT A: Definitions	#71 – Page 47	Does DHHS intend to use SCRIBBLES as an external system for document storage and management, or should the vendor propose a document storage solution?	The Workforce Registry will act as a repository and document management system for the EEB Unit. See Addendum 1 2.c) for details. Vendor may submit proposal with an alternate document management solution.
11	General		Does DHHS require multi-language application support across all three platforms? If so, what languages must be included in each application for users?	DCDEE requests English and Spanish at a minimum. This application should match the DCDEE public facing website setup. DCDEE public facing website offers Google Translate as a translation resource.
12	ATTACHMENT K: REGULATORY MODERNIZATION	COM 3 – Page 139	Please confirm whether DHHS requires the system to auto-calculate the QRIS based on interfaces and data entry, or if this will be manually calculated/assessed by a consultants/state worker with a combination of data integration and manual data entry.	Yes, DHHS requires the system to auto-calculate the QRIS based on interfaces, data entry and required algorithms. Authorized Users shall have ability to modify data if needed.
13	ATTACHMENT L: WORKFORCE REGISTRY	INF_7 – Page 147 WF_19 – Page 145 SFTP_REC_1 – Page 148	WF 19 specifies 'eligible enrollees can apply for grants' within the workforce registry. Please specify what types of grants and eligibility requirements would be directly managed within the workforce registry. Alternatively, please confirm if this is an interface with CCSA and the workforce registry would be utilized solely for tracking and reporting capabilities.	The Registry shall allow state staff to track and report on various grants such as Child Care and Development Block Grant (CCDBG) and others. This feature would be utilized solely for tracking and reporting purposes. DCDEE would receive the data from CCSA and update the Registry.

Question #	Solicitation Section	Solicitation Subsection	Vendor Question	Agency Response
14	ATTACHMENT M: NC PRE-K SPECIFICATIONS	PK_ADM_1 – Page 151 CHL_APP_9 – Page 152 PK_WF_2,11,20, 23 & 24 – Page 153	Will families use the Pre-K portal, or is this portal only for state and contracted agencies? If families use the Pre-K portal, please detail the functionality available within the portal for families. 2. Can DHHS provide a user manual or screenshots of the NC Pre-K legacy system?	Yes. Families will use Pre-K portal. Please refer to specifications applicable to Registration and Child Application for the portal functionality in page 151 and 152 of the RFP. Question 2: Attached link should suffice (https://ncchildcare.ncdhhs.gov/Home/DCDEE-Sections/North-Carolina-Pre-Kindergarten-NC-Pre-K). Three user manuals can be accessed via the website.
15	ATTACHMENT M: NC PRE-K SPECIFICATIONS	PK_WF_3 – Page 153	PowerSchool has a wide array of modules available. What part of PowerSchool's functionality is being used by the state?	Currently, there is no integration. This is a manual process. However, DCDEE is interested in knowing if the proposed solution has the ability to download data from PowerSchool to Excel or other document type(s) and upload it into NC Pre-K applications.
16	General		Could the state please share how many internal state users (including any state consultants) are expected to use this system? Similarly, how many childcare professionals and families are expected to utilize the solution's portals.	300+ internal users and 55,000+ childcare professionals.
17	page 5 and page 82		Can you clarify contract term? Page 5 describes 2 year term with one year optional but cost table on page 82 in appendix E has form that asks for information on a three year term with 2 additional one year terms as optional. Will cost be evaluated on contract term only or will it include contract term and the optional years?	Please refer to # 1.
18	page 23		How many total internal state users are there that will use the system? Page 23 describes concurrent users of 690 and capacity to handle up to 1380 users. Is 1380 the total number of users?	How many total internal state users are there that will use the system? See answer to #16. Page 23 describes concurrent users of 690 and capacity to handle up to 1380

Question #	Solicitation Section	Solicitation Subsection	Vendor Question	Agency Response
				users. Is 1380 the total number of users? 1380 is an estimate of the upper capacity of concurrent users the solution is to support with minimal performance degradation.
19	page 5		How many licensed child care providers organizations are there in the state of NC? How many child care providers apply for new applications annually? How many child care providers renew annually? And how long does the renewal term last?	How many licensed child care providers organizations are there in the state of NC? See response to # 6. How many child care providers apply for new applications annually? We currently do not track how many providers apply. How many child care providers renew annually? NA – 2 to 5 star licensed facilities must be reassessed every 3 years. And how long does the renewal term last? See response above.
20	Page 5		How many individual early child care professionals are there in the state? How many individual early child care professionals apply for new licenses annually? How many individual child care professionals renew annually? And how long does the renewal term last?	How many individual early child care professionals are there in the state? Response: See answer to #16. How many individual early child care professionals apply for new licenses annually? This is a moving target year to year. We cannot predict or estimate how many new people will enroll with the EES Unit and apply for new licenses. How many individual child care professionals renew annually? around 80 to 85 And how long does the renewal term last? Renewal terms are based on licensure types. Continuing licenses have a 5 year renewal term. Initial license have a 3 year renewal term and/or convert to a Continuing license at the end of the 3 years. Residency licenses last for 1 year and can be renewed up to 2 additional years (at the end of the 3rd year it needs to

Question #	Solicitation Section	Solicitation Subsection	Vendor Question	Agency Response
				<p>convert to an Initial or Continuing license). Provisional BK add-on licenses are a 1 year renewable license for up to 5 years.</p> <p>Note: EES only caters to Lead Teacher. We are speaking about childcare professionals that include several different categories. Lead teacher is only one.</p>
21	page 20 3.5.5 Data Conversion and Migration		<p>Can you describe the amount and type of data that will need to be migrated to the new solution? ...data volume vs file volume....total number of GB or terabytes of each.....is it structured data or Unstructured?</p> <p>Does your organization anticipate storing CJI data as a part of the cloud-based solution?</p> <p>Can a solution be proposed whereby CJI data lives in an on-premise solution at a data center and is integrated with the cloud-based solution being proposed using tokenization to ensure Cloud Service Provider (CSP) personnel have no access to the CJI data? With this approach, CJI data would not be stored in a cloud database but would provide a pointer from a cloud database to the CJI data stored in the data center enabling your organization users to securely access that data.</p> <p>We further assume that the CSP will not need to comply with the CJIS compliance requirements. Please confirm.</p>	<p>Both structured and unstructured.</p> <p>Workforce Registry: Approximately 200GB. The WORKS database houses data for education, qualification, and licensure for 10 positions including Teachers, Lead Teacher, FCCH Providers, Program Coordinator, Group Leader, DPI Teacher, DPI Teacher Assistant and Administrator (EC, SA, DPI).</p> <p>NC Pre-K: Approximately 50 GB but could be more depending on size of archived data. The NC Pre-K database houses data for Child, Sites, Classrooms, Teacher licensure and education, Contracting Agencies and Budget.</p> <p>Regulatory: Approximately 30 GB.</p> <p>Yes, as long as government cloud is managed by NCDIT. Further, for compliance requirements please refer to the CJIS Security Policy document. (https://cjin.nc.gov/infoSharing/Presentations/CJIS%20Security%20Policy%20v5%20107132012-ns[1].pdf)</p>

Question #	Solicitation Section	Solicitation Subsection	Vendor Question	Agency Response
22	page 64 III) (5)		<p>Does your organization anticipate storing CJI data as a part of the cloud-based solution?</p> <p>Can a solution be proposed whereby CJI data lives in an on-premise solution at a data center and is integrated with the cloud-based solution being proposed using tokenization to ensure Cloud Service Provider (CSP) personnel have no access to the CJI data? With this approach, CJI data would not be stored in a cloud database but would provide a pointer from a cloud database to the CJI data stored in the data center enabling your organization users to securely access that data.</p> <p>We further assume that the CSP will not need to comply with the CJIS compliance requirements. Please confirm.</p>	Response: See response to question 21.
23	Page 22 2.f.		<p>Cloud Services Provider (CSP) uses commercially reasonable efforts to make its on-demand services available to its customers 24/7, except for planned downtime, for which the CSP gives customers prior notice, and force majeure events. While availability SLAs can be negotiated in a contract, the calculation is measured quarterly and not monthly.</p> <p>Can your organization please adjust this requirement and specify that the SLA requirements can be negotiated based on the Service provider chosen?</p>	Vendor may submit their standard SLA. However, the SLA will be finalized during contract negotiations with finalists.
24	7.8 Security and Background Checks		<p>We assume this only applies to contractor personnel that are performing the solution implementation services and not the Cloud Service Provider (CSP) personnel that are hosting the solution.</p> <p>For example, CSP engages the services of a background screening vendor to conduct background checks on employees at the time of hire. The CSP also performs background investigations in certain foreign countries. The scope of these checks is subject to local laws in the jurisdictions in which the employee is hired. Can your organization please modify this requirement accordingly? Does your organization agree with this interpretation of this requirement? If your organization mandates that CSP's also needing to meet this requirement, will your organization be willing to sponsor and pay for these background checks?</p>	This is State requirement for which DHHS cannot provide an exception. This can be discussed with State CIO during negotiations.
25	Immediate Breach Notification		<p>The Cloud Service Provider (CSP) is a service provider and your organization would be one of hundreds of thousands of customers using the service. CSP can contractually commit to incident</p>	This is State requirement for which DHHS cannot provide an exception. This can be discussed with State CIO during negotiations.

Question #	Solicitation Section	Solicitation Subsection	Vendor Question	Agency Response
			<p>response reporting timeframes in a customer contract. One component driving the timeframes are the CSP's ability to communicate to a wide customer base in the event of an incident. In a multi-tenant cloud environment, the CSP could be reporting to thousands of customers if there is a security incident impacting multiple customers. CSPs utilize one incident response process for all customers. Utilizing one approach allows for scalability and ease of operations.</p> <p>Additionally, due to the nature of the CSP's service, the CSP can only report confirmed breaches, not attempted, suspected, threatened, or foreseeable breaches. As a multitenant environment, an attempted breach against another tenant would not be reported to your organization.</p> <p>In the event of a security breach and if negotiated in the agreement, the CSP can notify your organization identified points of contact. The CSP cannot notify affected parties because the CSP does not view customer data. The CSP is responsible for maintaining access in terms of performance and availability to the data. The data is owned by the customer. As such, we would like to request the requirements for breach notifications should align with the existing CSP reporting requirements that also align with FedRAMP and request that your organization change this requirement.</p>	
26	Liquidated Damages		<p>Your organization will have full control of the data they store within the Salesforce Services. Salesforce does not classify Customer Data. All information that has been electronically submitted by customers to the Salesforce Services is considered "Customer Data" and is protected as confidential. Permitted access to the production environment infrastructure is restricted to a very limited number of full-time Salesforce employees required to manage the service. These Salesforce employees do not have login access to customer's instances (org), and because of Salesforce's multi-tenant infrastructure, they do not see customer data in an assembled manner.</p> <p>Our interpretation is that this would primarily apply to the System Integration personnel (its employees and subcontractors) that would be directly performing the solution implementation services and could have direct access to your organization's data.</p> <p>Would your organization be willing to make an adjustment to the breach liability and related costs and remove "amount determined to be adequate by the agency" to allow for negotiation of these</p>	No.

Question #	Solicitation Section	Solicitation Subsection	Vendor Question	Agency Response
			requirements to refine the parameters, guidelines, and associated costs. Typically breach liability and related costs are considered indirect damages as they are unknowable and unpredictable. As such, they are a source of risk to a provider and the provider needs to be able to further assess such risk after consideration and discussion with your organization.	
27			It indicates in Section 7.2 on page 34 that Vendors are to provide "b) a written statement" from a CPA. Would evidence that a Vendor is currently working with MCOs in NC and has serviced these entities for 15 years serve as a substitute for this requirement?	No
28			As part of your redundancy plan are you wanting a crosscheck of electronic documents versus the paper documents. Is it necessary to reference (or store) these paper documents. Does the redundancy plan include an electronic record (scan) of the existing paper documents?	Crosscheck: Yes. DCDEE will not be storing paper documents. Once the documents are scanned into the Registry the expectation is to store the documents as per Division's records management policy. Yes, all documents will be electronically stored and managed within the Registry. DCDEE does want this system to interface with the DHHS ITD's document management system (documents stored on a file server). The solution will need to support the Division's records management schedule.

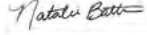
Failure to acknowledge receipt of this addendum may result in rejection of the response.

Check ONE of the following options:

- ☒ Bid has not been mailed. Any changes resulting from this addendum are included in our bid response.
- ☐ Bid has been mailed. No changes resulted from this addendum.
- ☐ Bid has been mailed. Changes resulting from this addendum are as follows:

Execute Addendum:

Offeror: Accenture LLP

Authorized Signature: 

Name and Titled (Typed): Natalie Batten, Managing Director

Date: August 17 2023



Solicitation Addendum

Solicitation Number: 30-23189

Solicitation Description: DCDEE – Workforce Registry and NC Pre-K and Regulatory System Replacement

Solicitation Opening Date and Time: August 17, 2023
2:00 PM EST

Addendum Number: 2

Addendum Date: August 9, 2023

Contract Specialist or Purchasing Agent: Jillian Kennedy, Contract Specialist
Jillian.kennedy@dhhs.nc.gov

1. Vendor must return one properly executed copy of this addendum with bid response or prior to the Bid Opening Date/Time listed above.
2. The solicitation is hereby modified as follows:
 - a) Section 1.0 **ANTICIPATED PROCUREMENT SCHEDULE** on page 4, the “Offer Opening Deadline” shall be replaced with the following:
August 17, 2023 at 2:00pm Eastern
 - b) Attachment Q -MMM on pages 171-173 shall be replaced with the following:
Attachments Q-MMM are made available through the Ariba system and are attached to Addendum 2.

Failure to acknowledge receipt of this addendum shall result in rejection of the response.

Check ONE of the following options:

- ☒ Bid has not been mailed. Any changes resulting from this addendum are included in our bid response.
- ☐ Bid has been mailed. No changes resulted from this addendum.
- ☐ Bid has been mailed. Changes resulting from this addendum are as follows:

Execute Addendum:

Offeror: Accenture LLP

Authorized Signature: 

Name and Titled (Typed): Natalie Batten, Managing Director

Date: August 17, 2023



Section r)

Draft Deliverables

r) Draft Plans

Draft Project Management Plan, draft Project Schedule, draft Staffing Plan, draft Service Level Agreement, and draft Vendor Operations and Maintenance Phase Staffing Plan.
Please refer to Attachment J: Minimum Content for Project and O&M Deliverables.

Table of Contents

1.0 Draft Project Management Plan	4
A. Project Background.....	4
B. Project Objectives	4
C. Project Success Criteria & Contingency	5
D. Project Assumptions & Constraints	6
E. Project Scope.....	7
F. Project High-Level Timeline.....	7
G. Project Deliverables.....	7
H. Project Management Methodology & Approach	11
I. Entrance & Exit Criteria for Specific Project Sprint/Cycles/Modules/Milestones	36
J. Status Reporting & Mechanisms.....	37
K. Monitoring & Control Mechanism & Corrective Plan Notification.....	38
L. Technical Approach & Transition Management	39
M. Organization Information	40
N. Knowledge Transfer Strategy.....	40
O. Documented Deliverables & Record Management Approach.....	42
2.0 Draft Vendor Project Schedule.....	43
3.0 Draft Vendor Staffing Plan.....	44
A. Staffing Plan.....	48
B. Staffing Plan by phase/stage.....	52
C. Roles and Responsibilities	57
D. Organization Chart.....	68
E. Skills required for NCDHHS staffing resource	69
F. Plan for resource turnover	69
4.0 Draft Service Level Agreement	71
1. Introduction.....	71
2. Definitions.....	72
3. Measurement and Calculation	73
4. Reporting.....	73

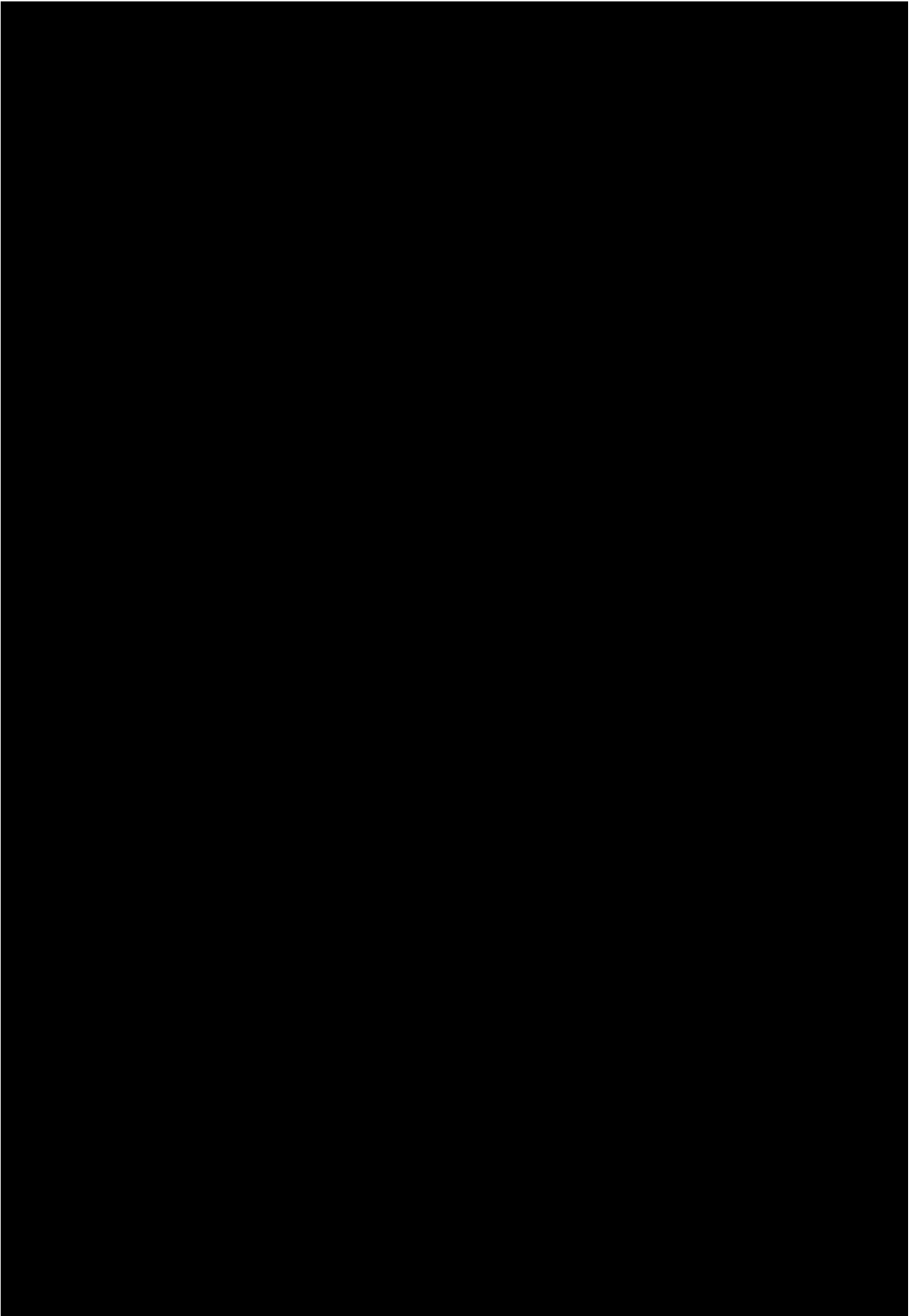
5. Initial Measurement and Burn-in Period.....	73
6. Service Level Default.....	73
7. Service Level Credits.....	74
8. Excused Performance	74
9. Earn-back Credits.....	75
10. Measurement Tools.....	75
11. Service Level Modifications	76
12. Low Volume.....	76
13. Solution Operations Key Areas.....	76
14. Attachment 1	81
15. Attachment 2	83
5.0 Draft Operations and Maintenance Phase Staffing Plan	96
A. Purpose/Description.....	96
B. O&M Staffing Plan.....	97
C. O&M Matrix of required skills/roles for each resource, O&M Roles and Responsibilities (and required skills for NCDHHS roles)	102
E. O&M Organization Chart.....	106
F. O&M Other resources available to the Agency	106

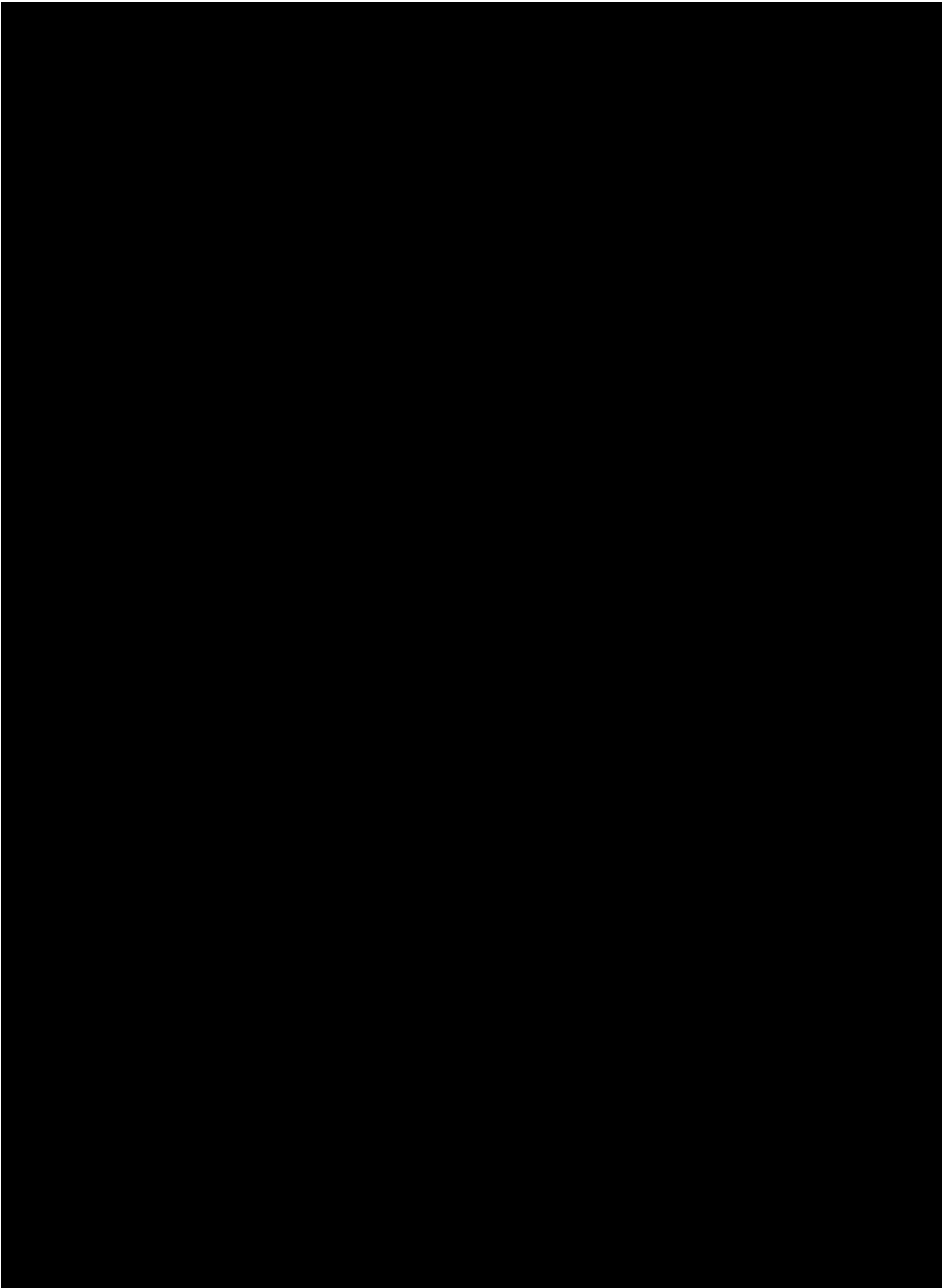
1.0 Draft Project Management Plan

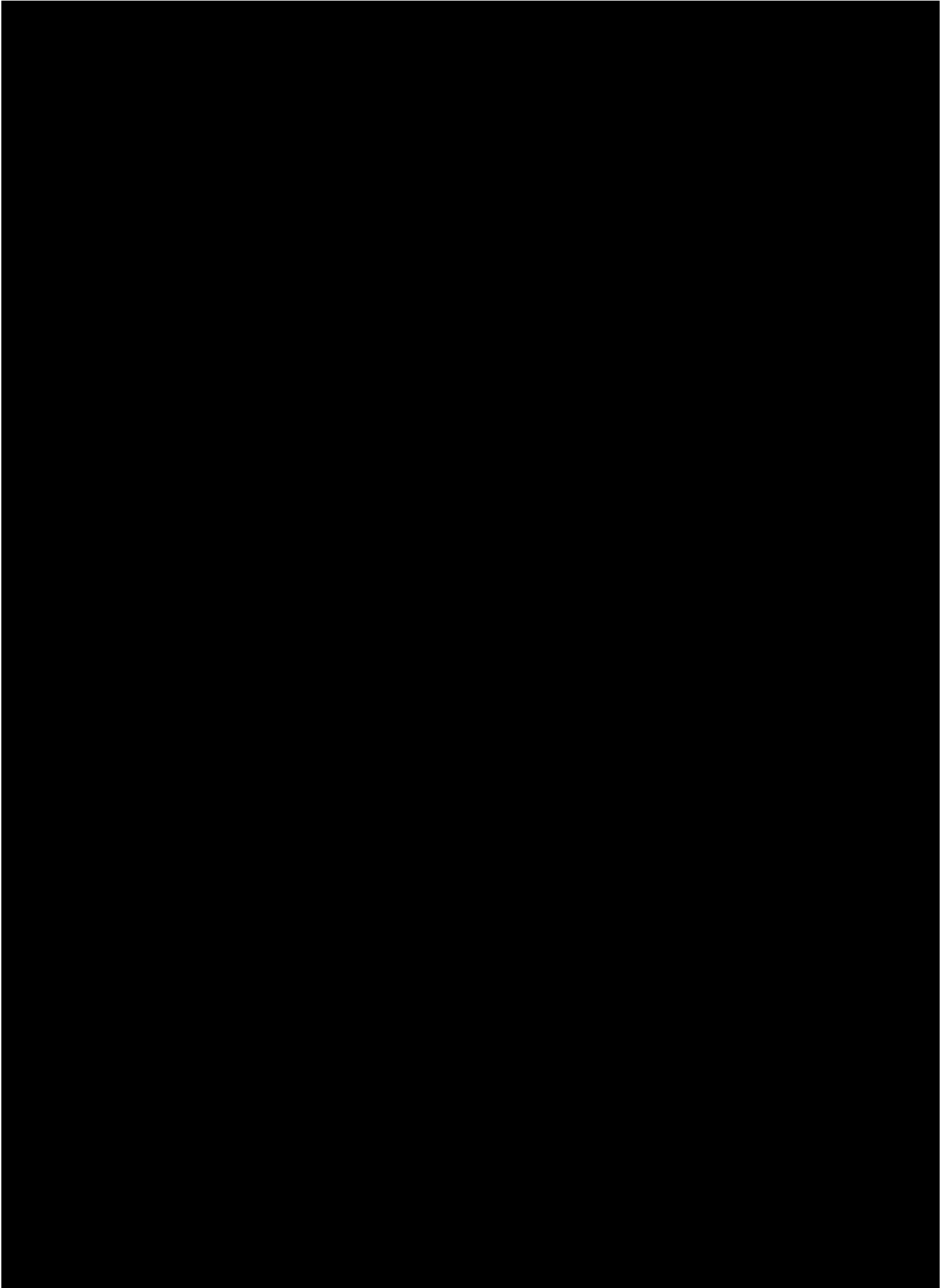
The Vendor Project Management Plan describes how the Vendor's engagement during the Project Execution will be executed, monitored, and controlled.

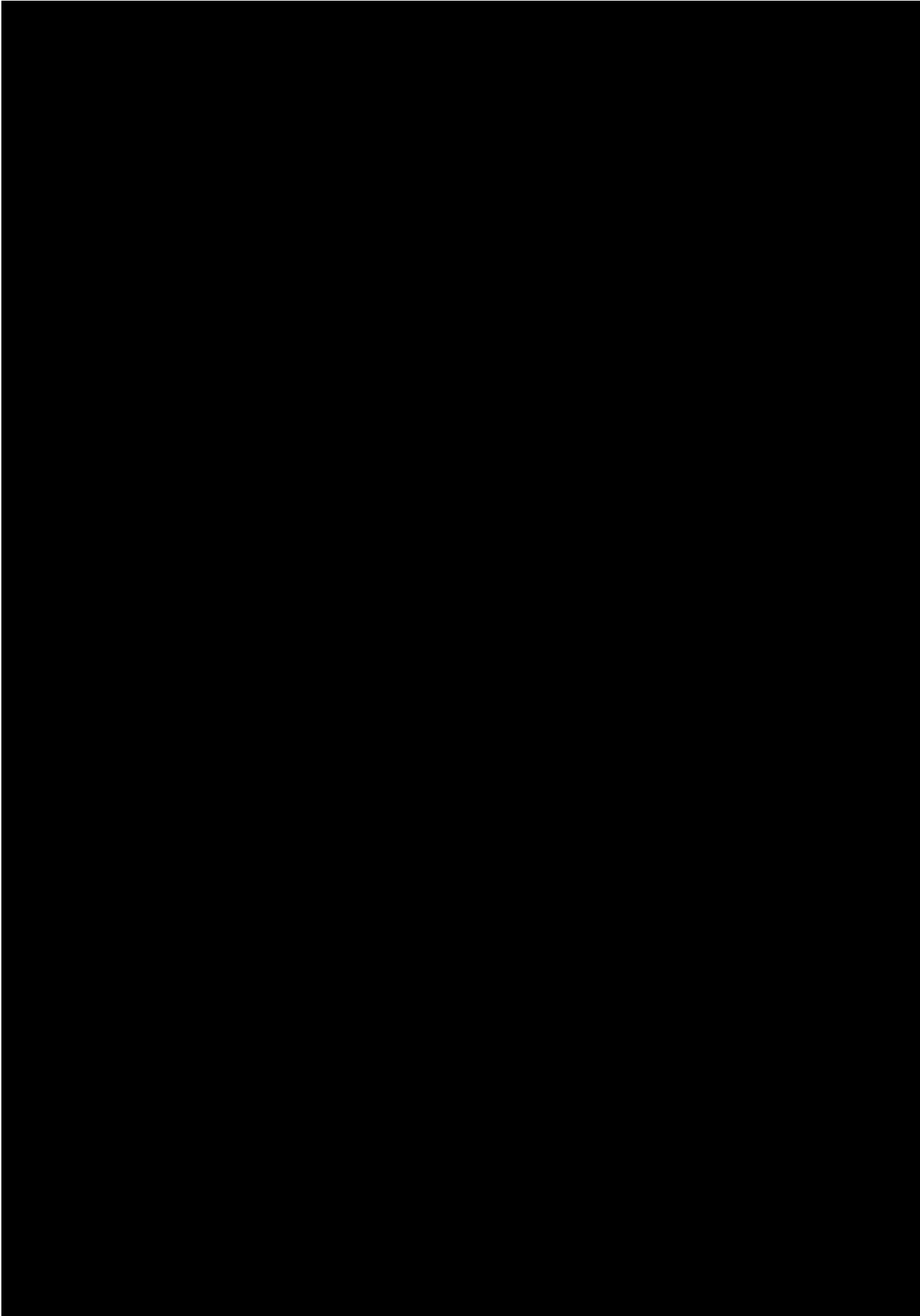
Minimum Content:

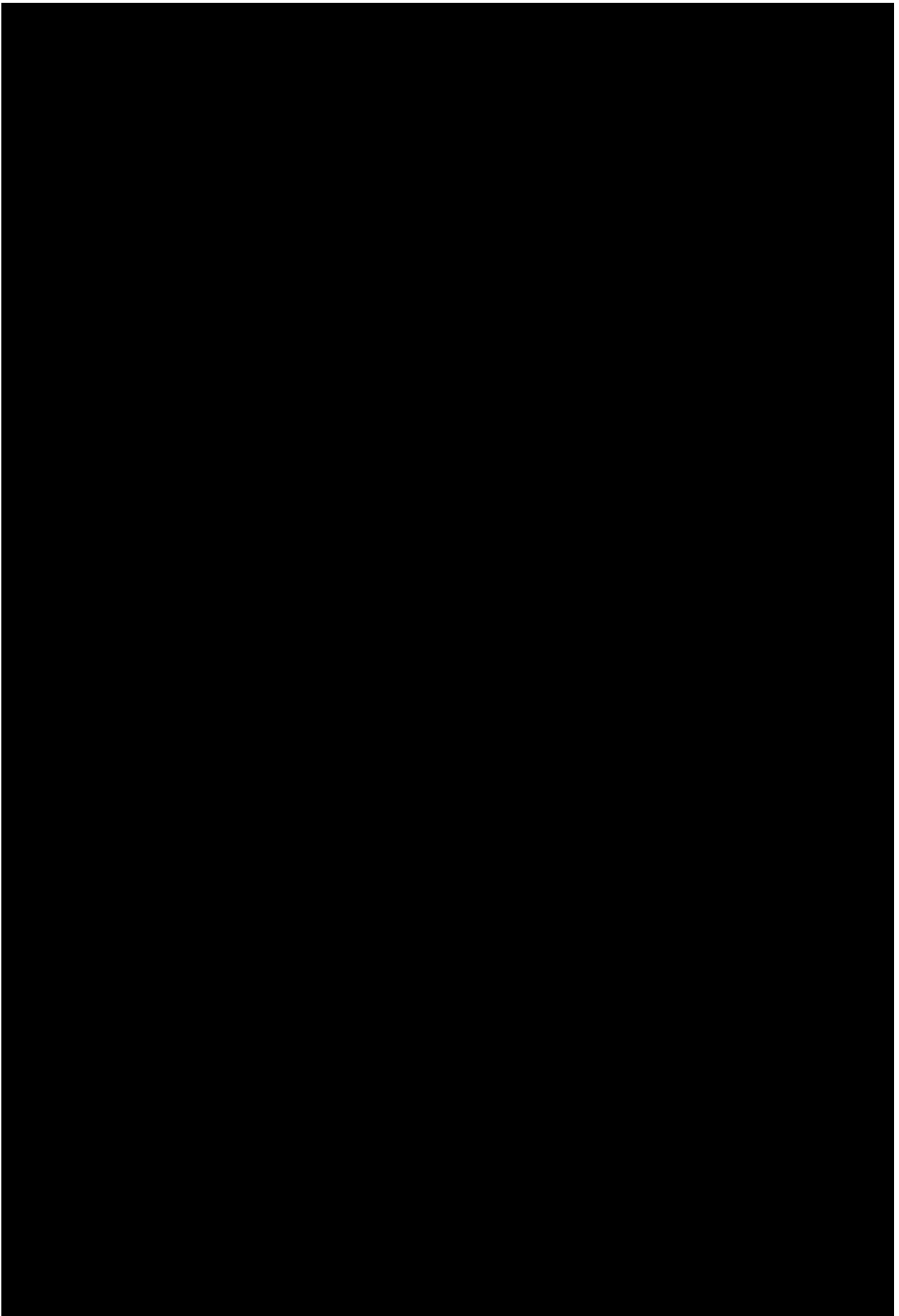
- Project background;
 - Project objectives;
 - Project success criteria and contingencies;
 - Project assumptions and constraints;
 - Project scope;
 - Project high-level timeline;
 - Project Deliverables;
 - Project management methodology and approach;
 - Entrance and exit criteria for specific project Sprint Cycles/Modules/Milestones;
 - Status reporting requirements and mechanisms, including update of Vendor Project Schedule progress;
 - Monitoring and control mechanisms and corrective plan notification;
 - Technical approach, including transition management;
 - The organizational information, including organizational chart that reflects roles and responsibilities for Vendor and subcontractors (if applicable)
 - Knowledge transfer strategy; and
 - Documentation Deliverable and record management approach
-

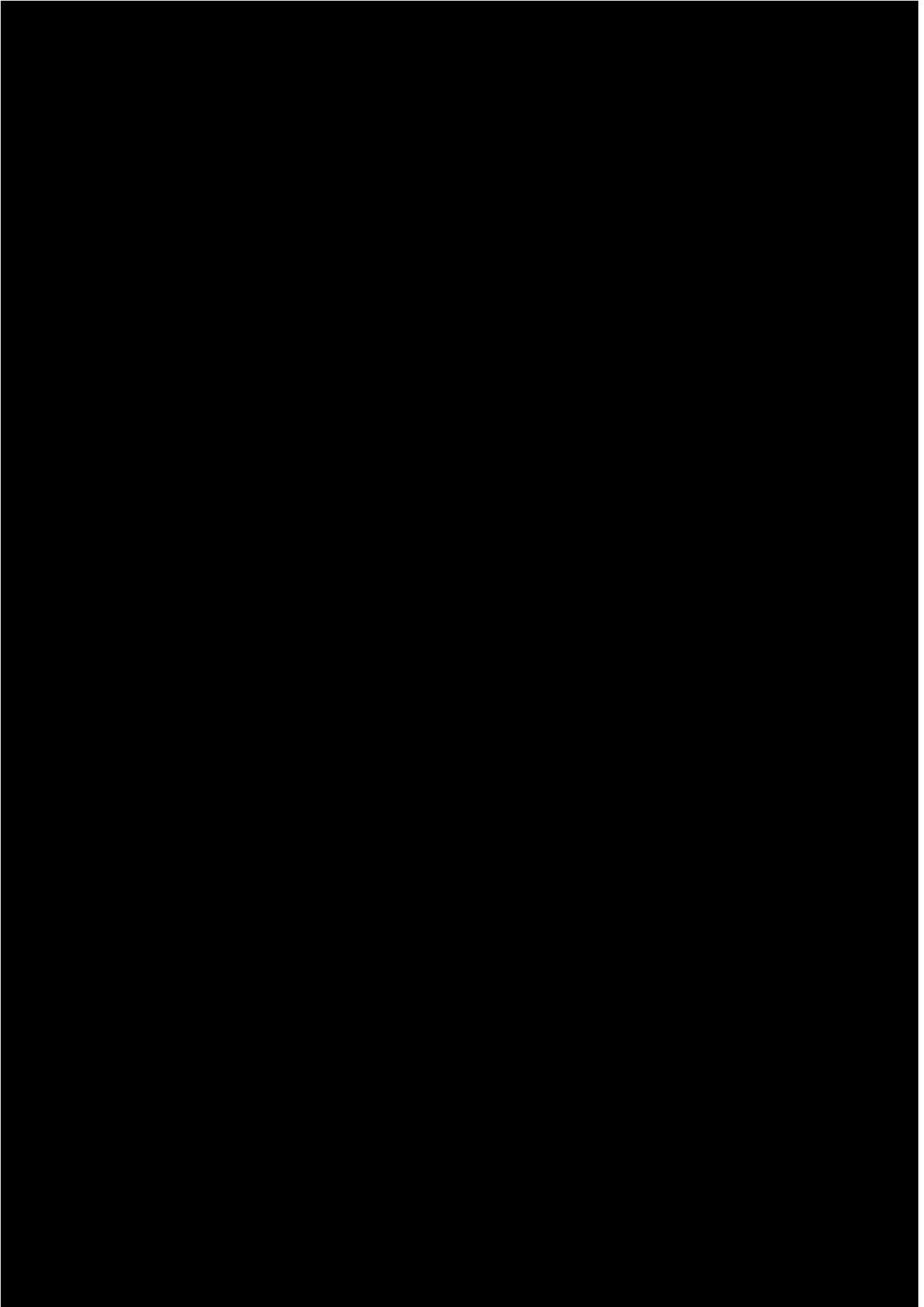




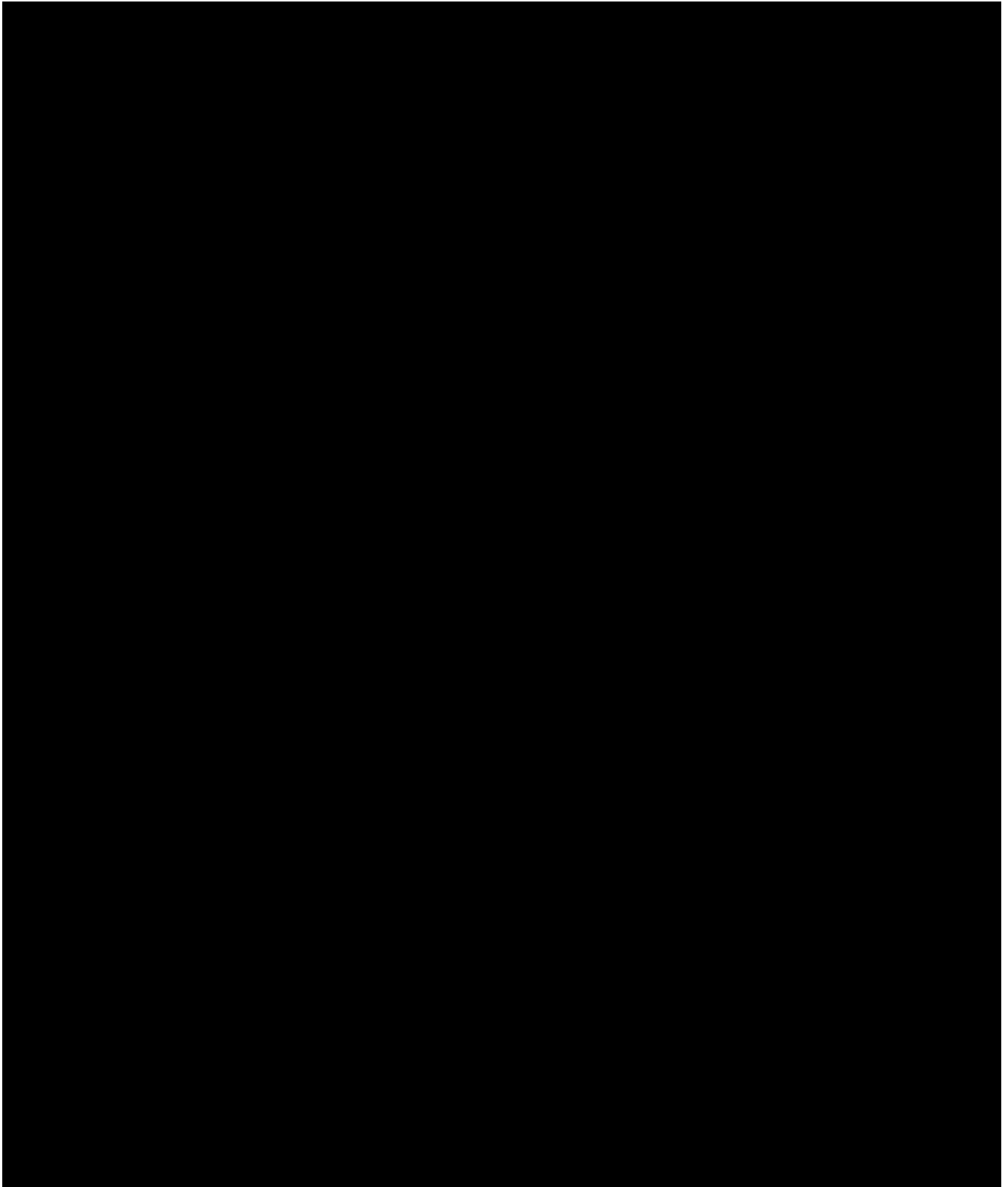


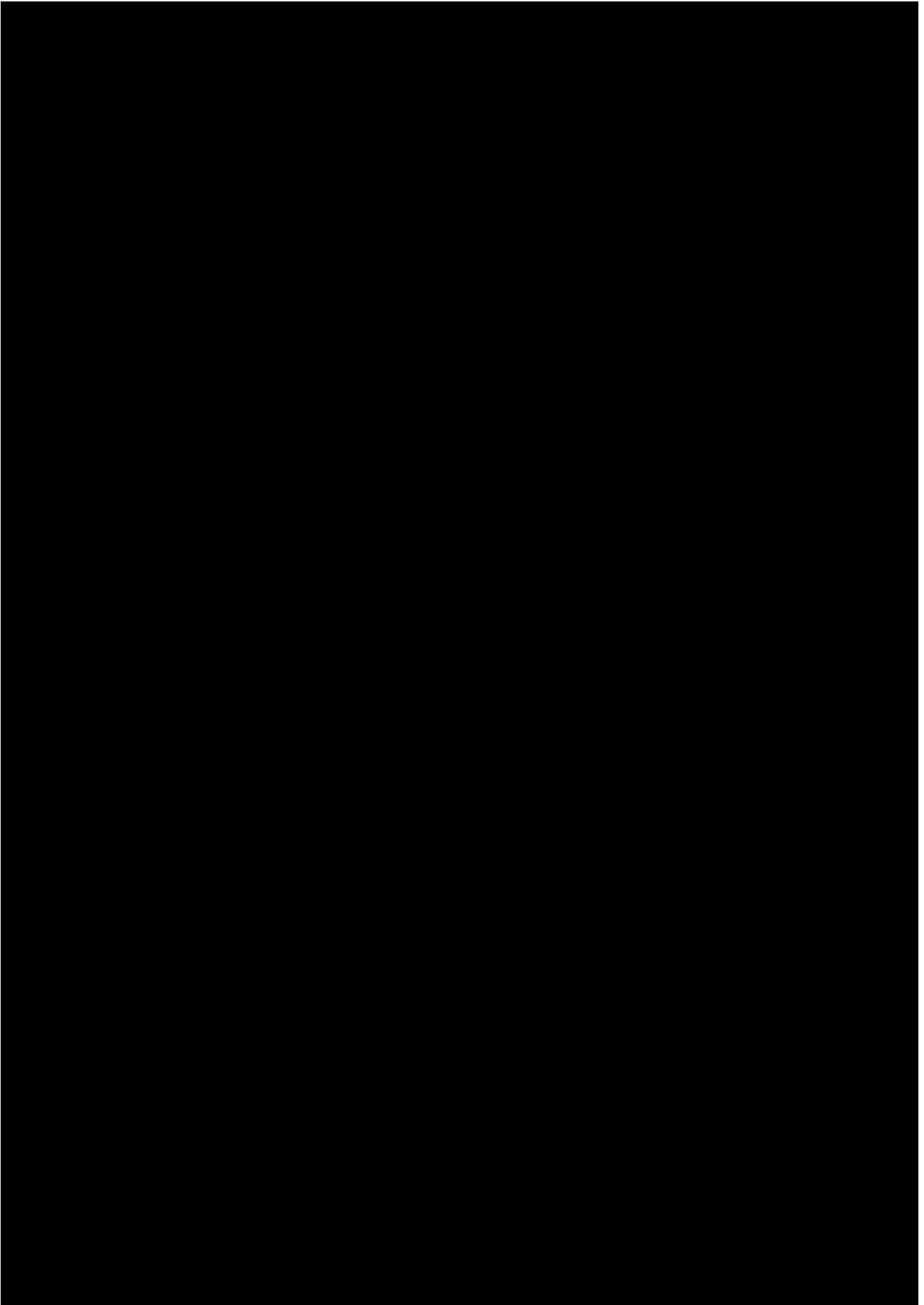


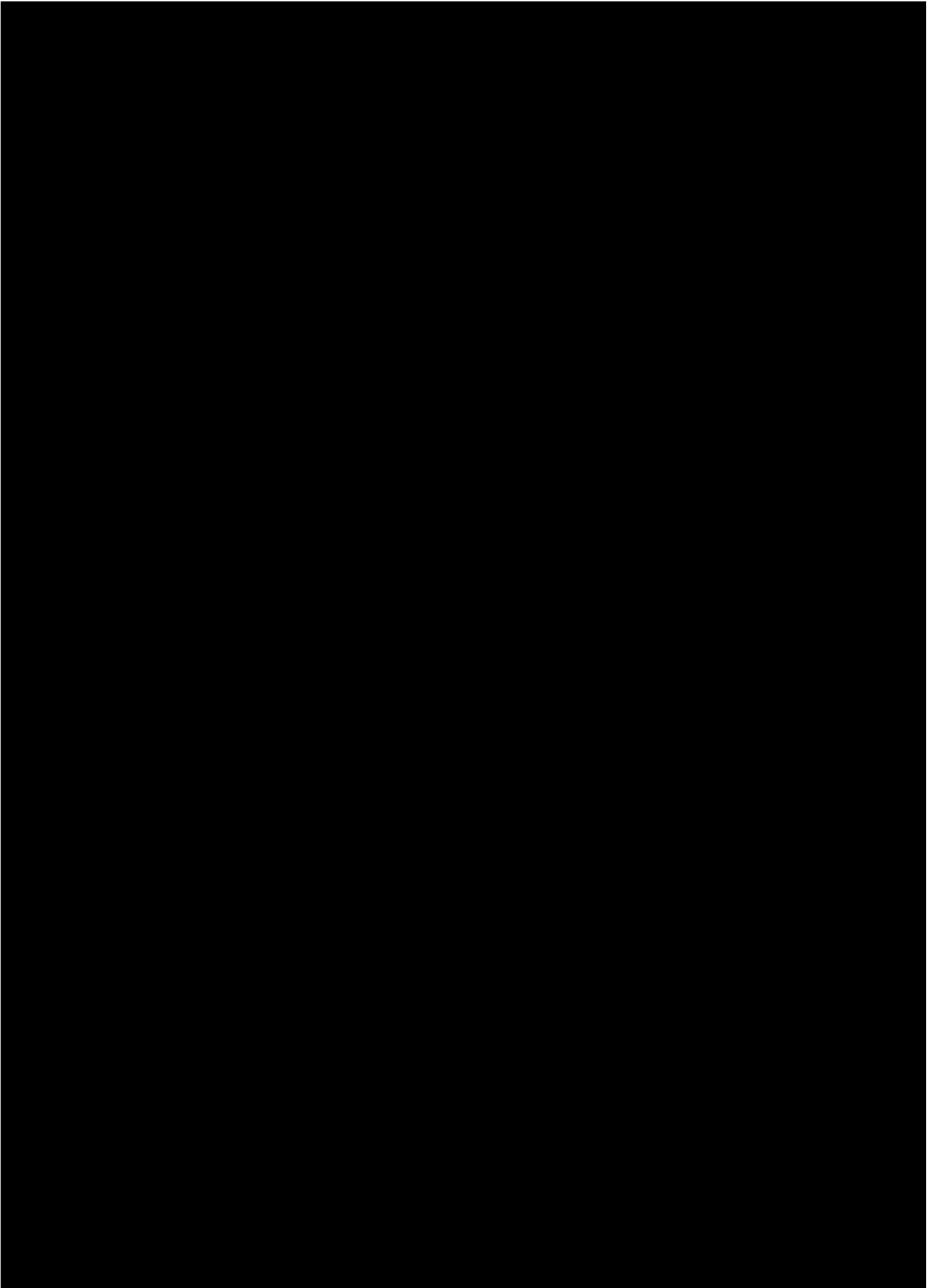


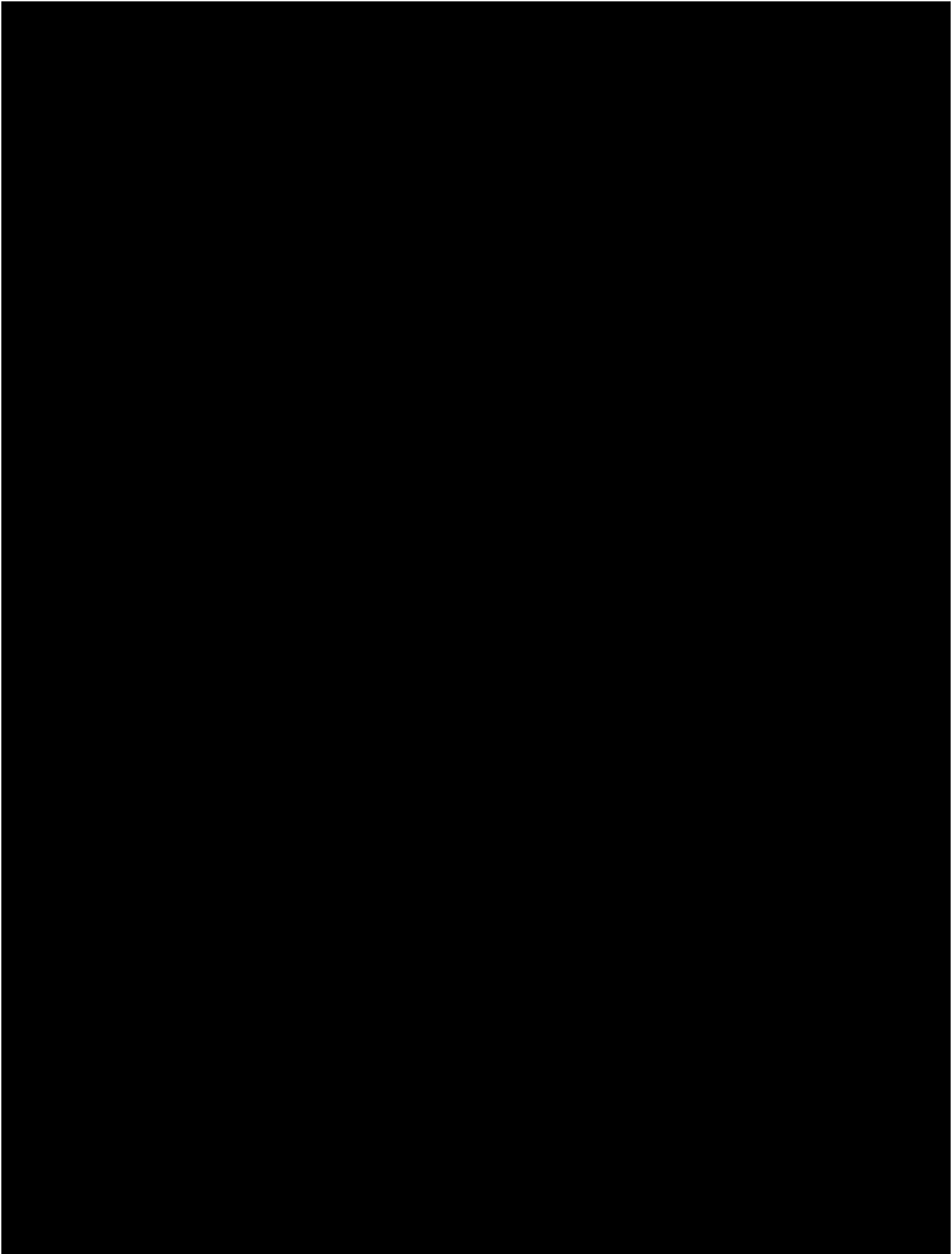


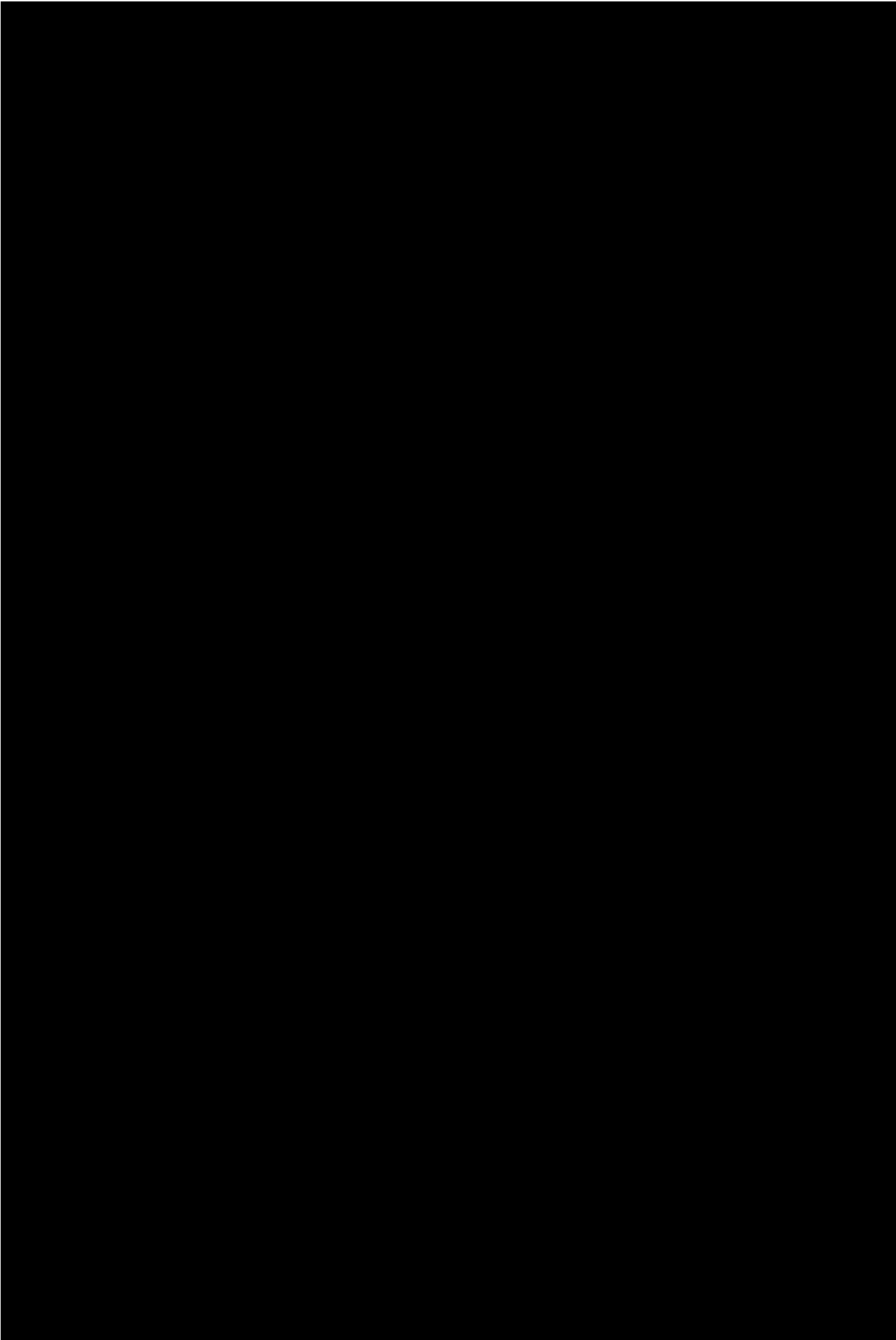
H. Project Management Methodology & Approach

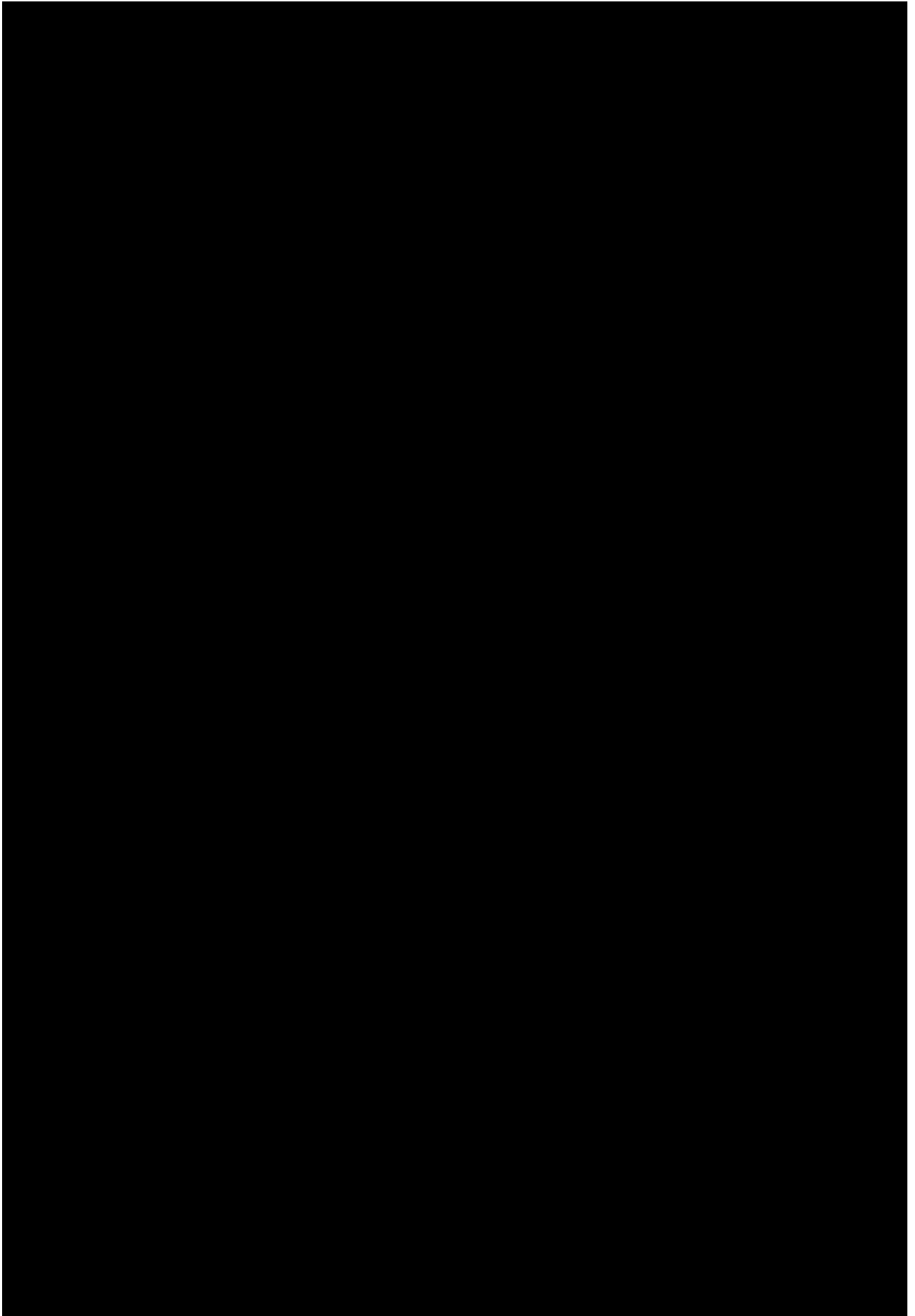


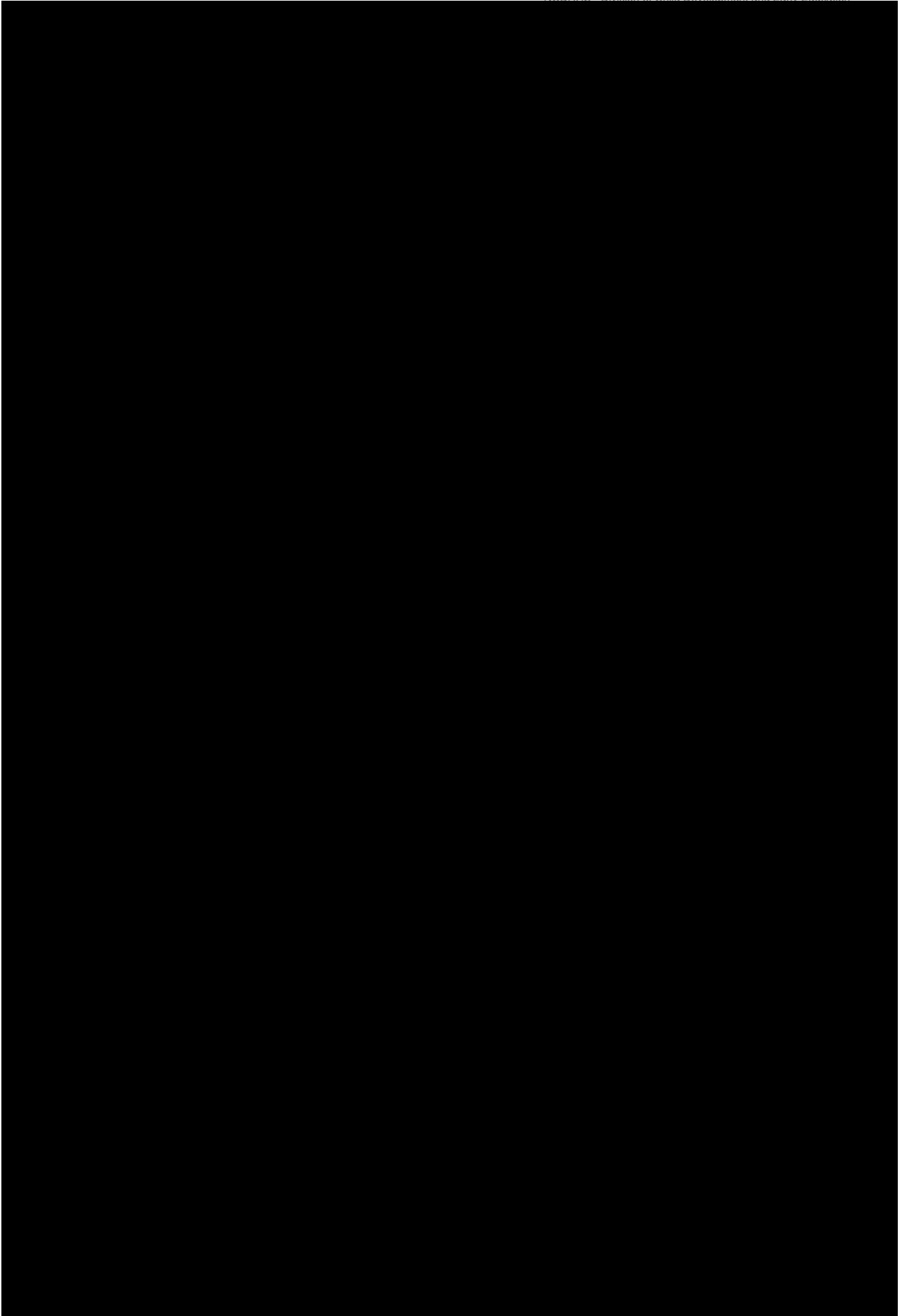


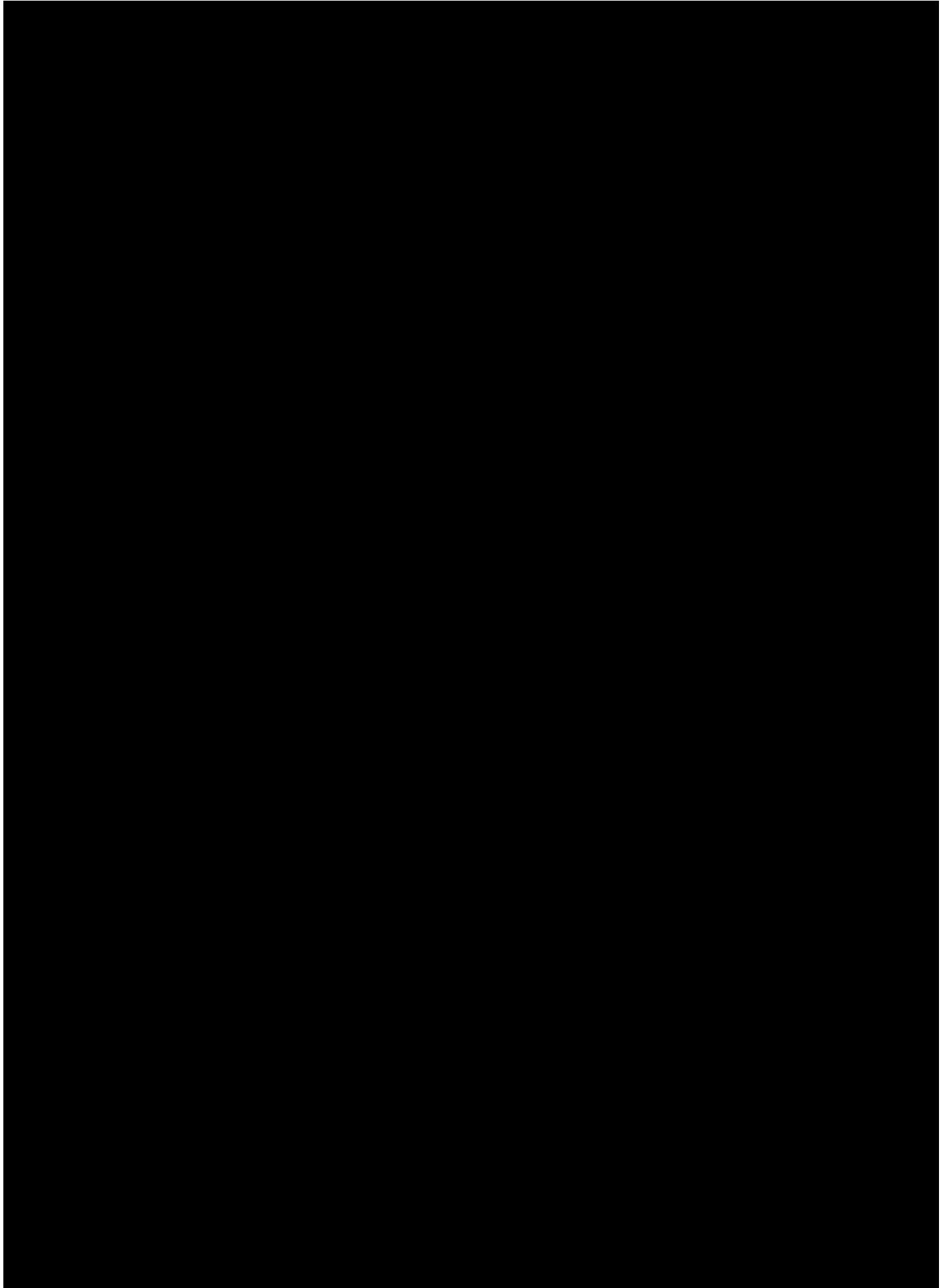


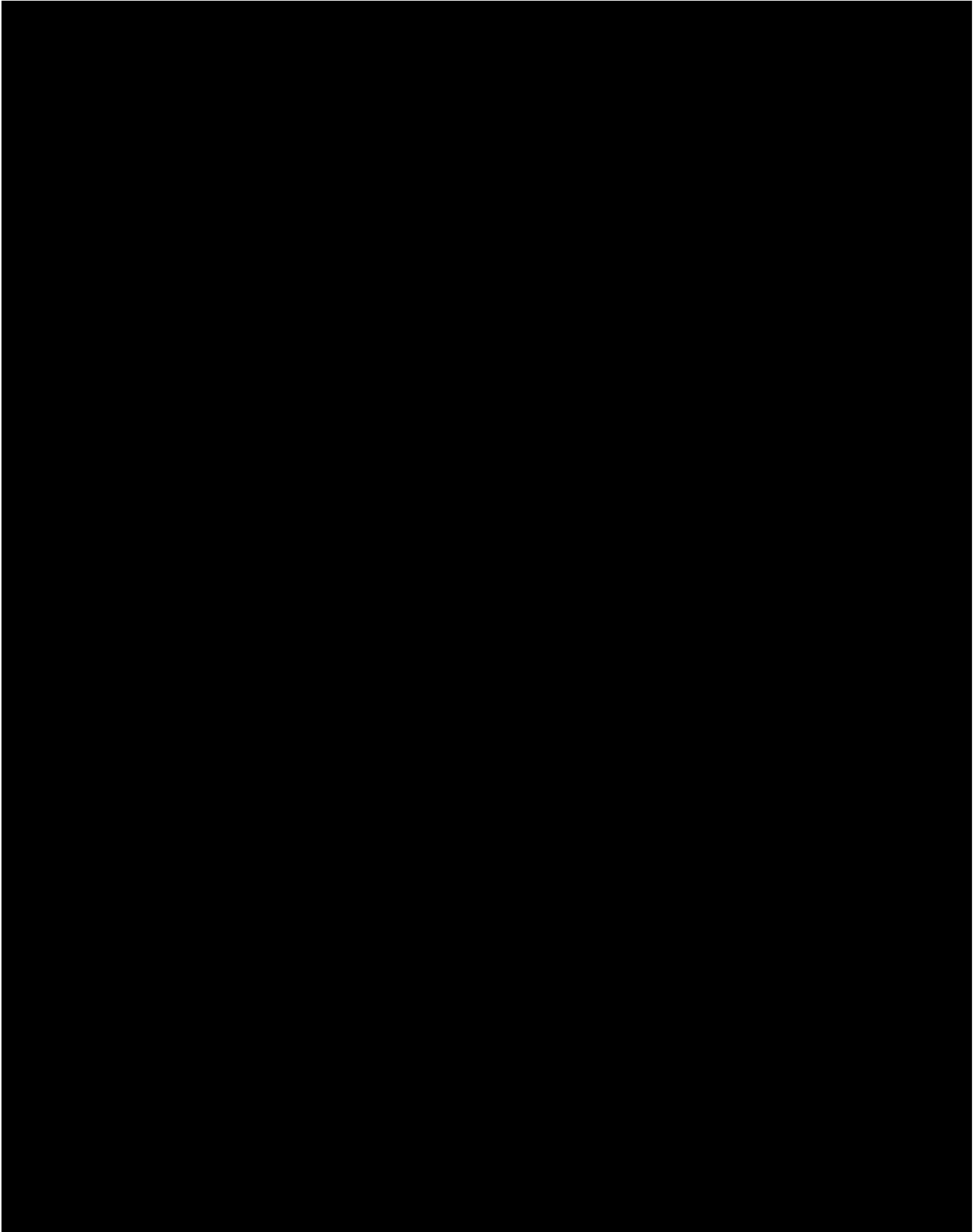


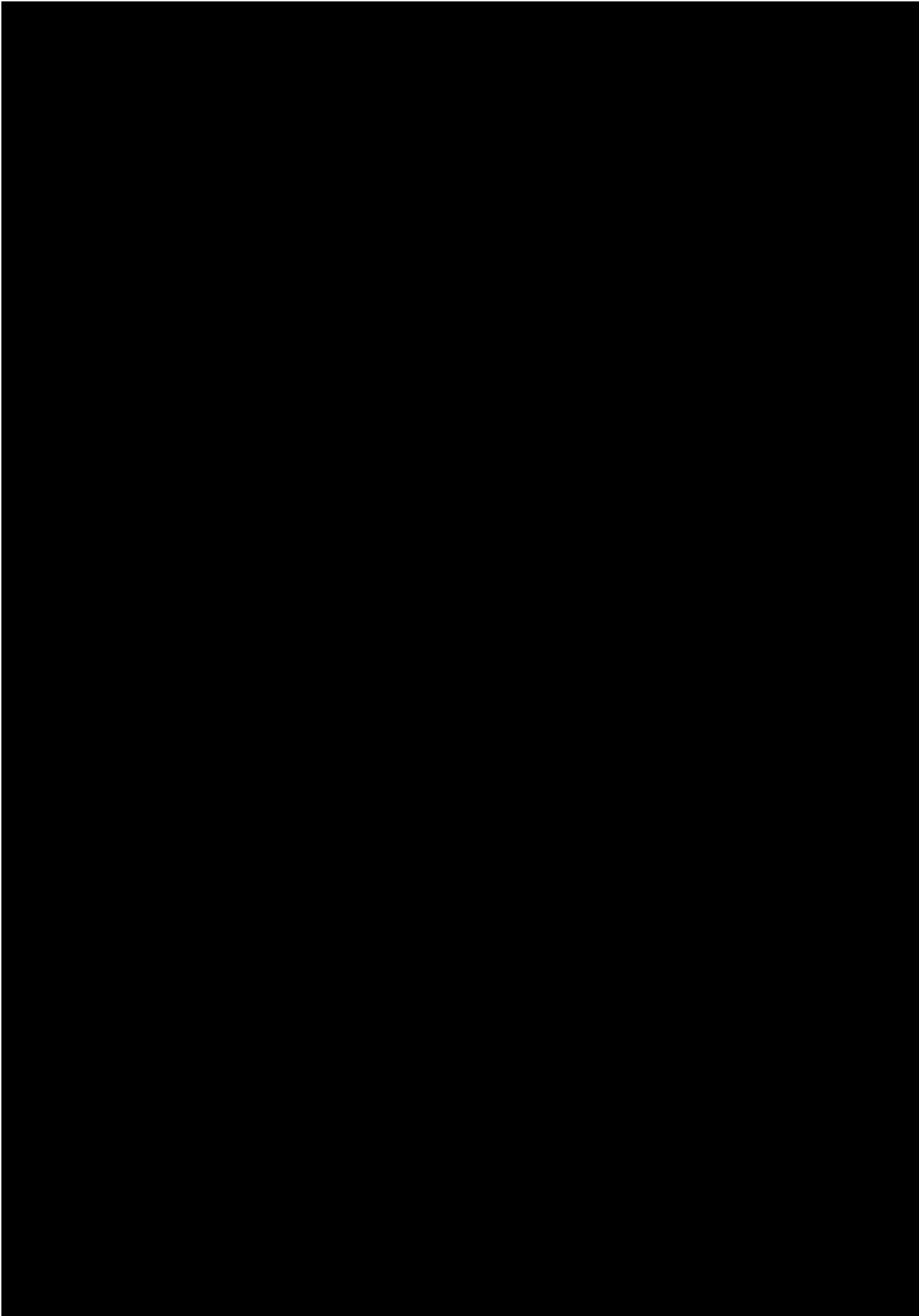


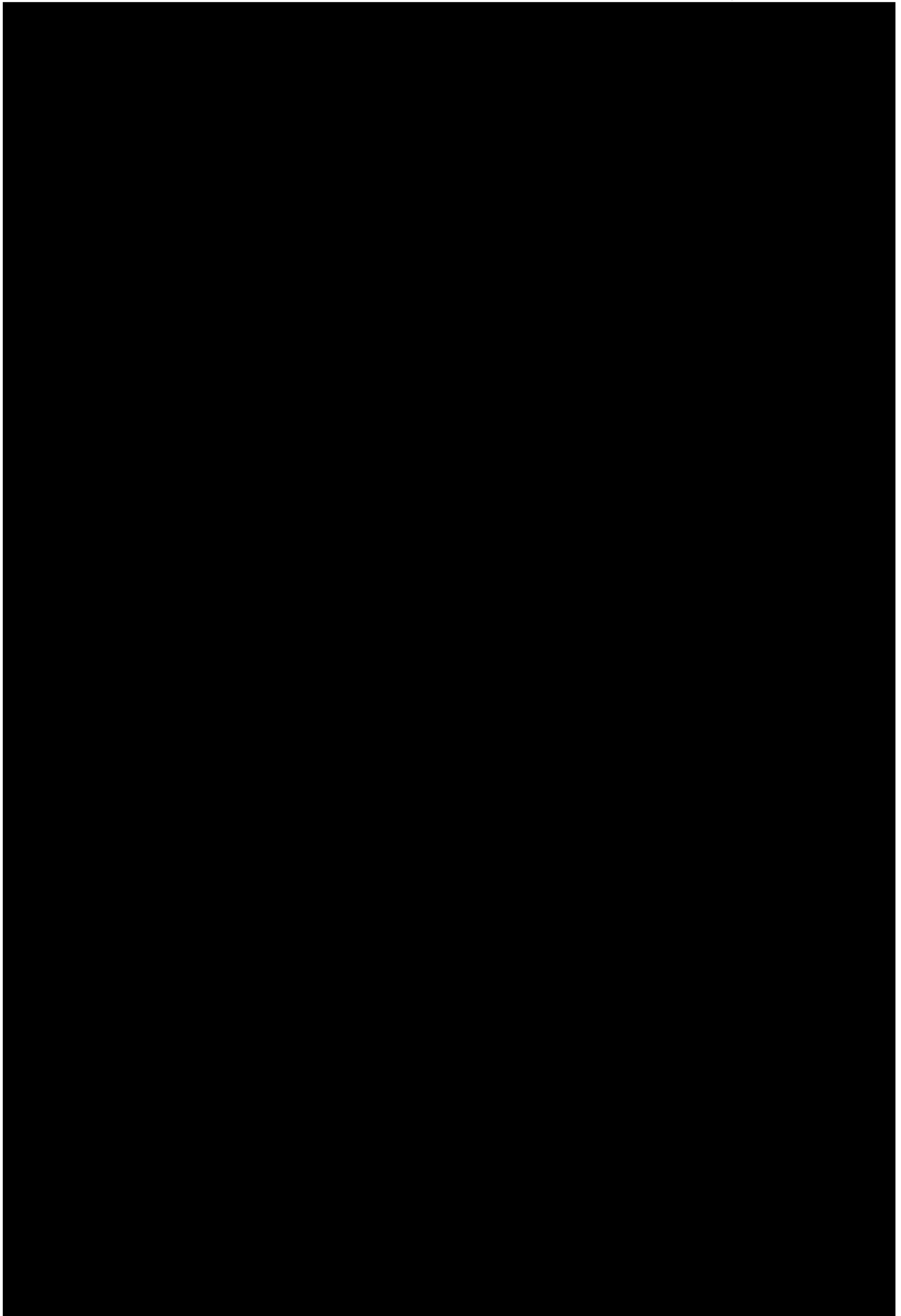


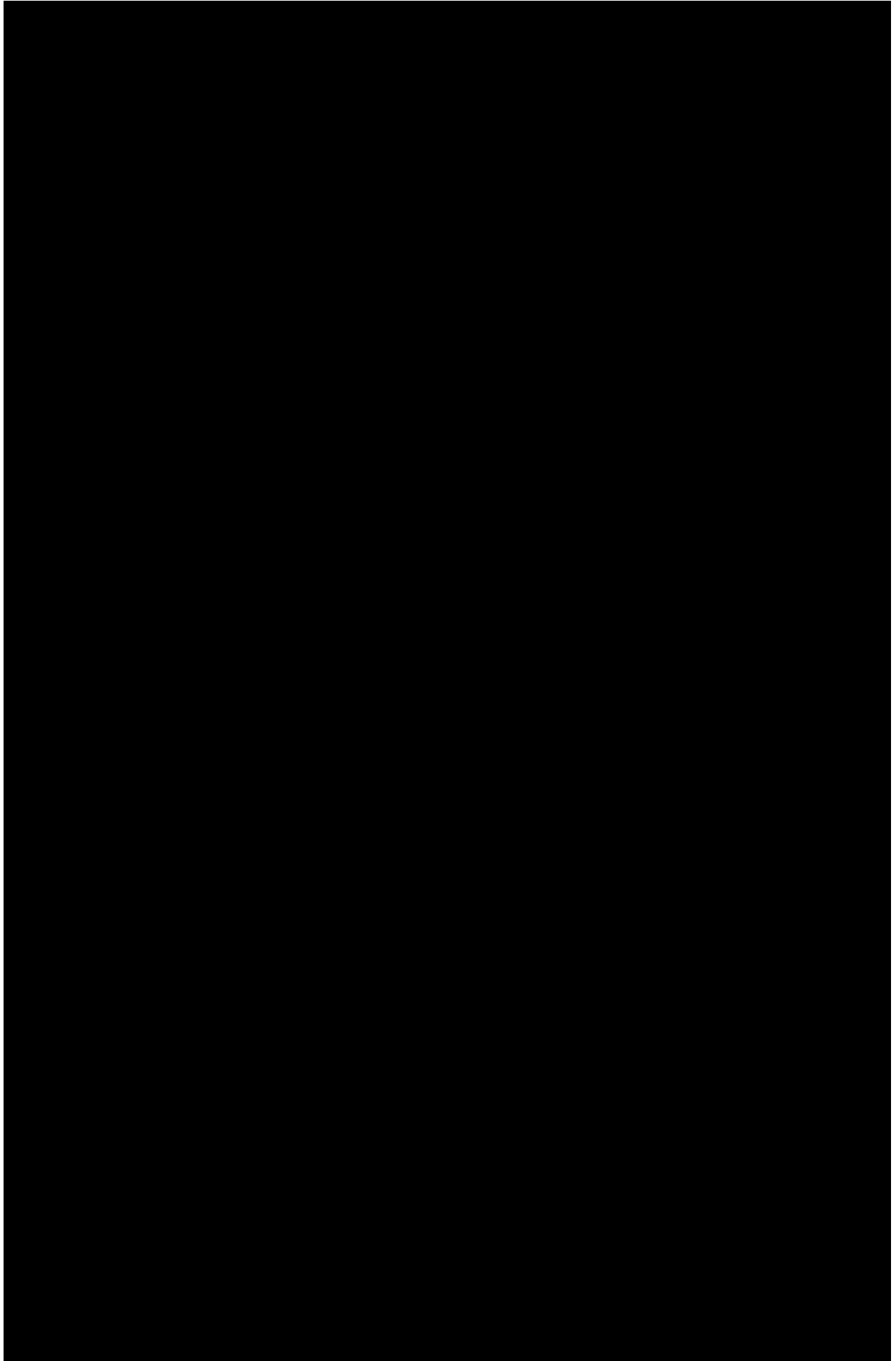


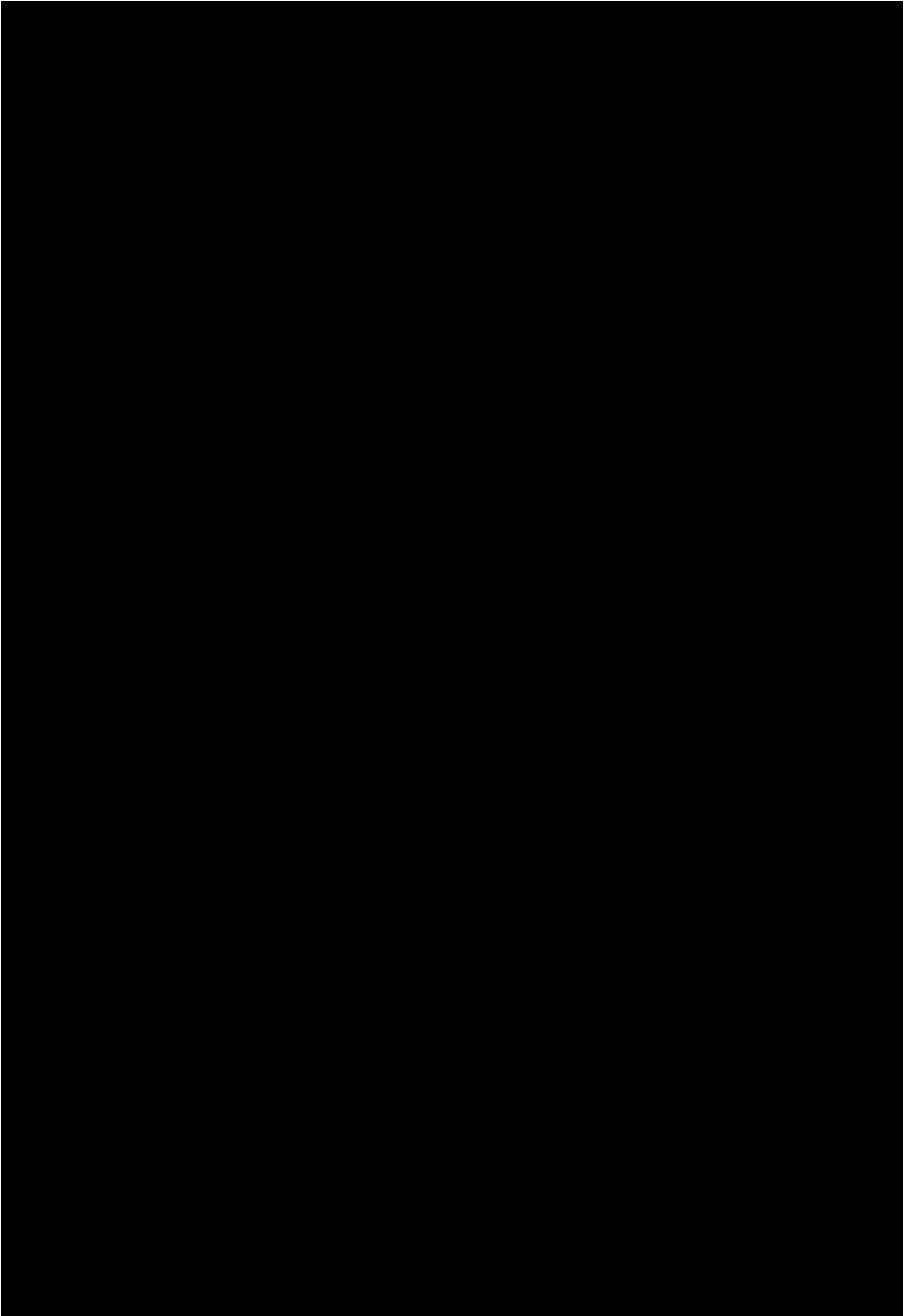


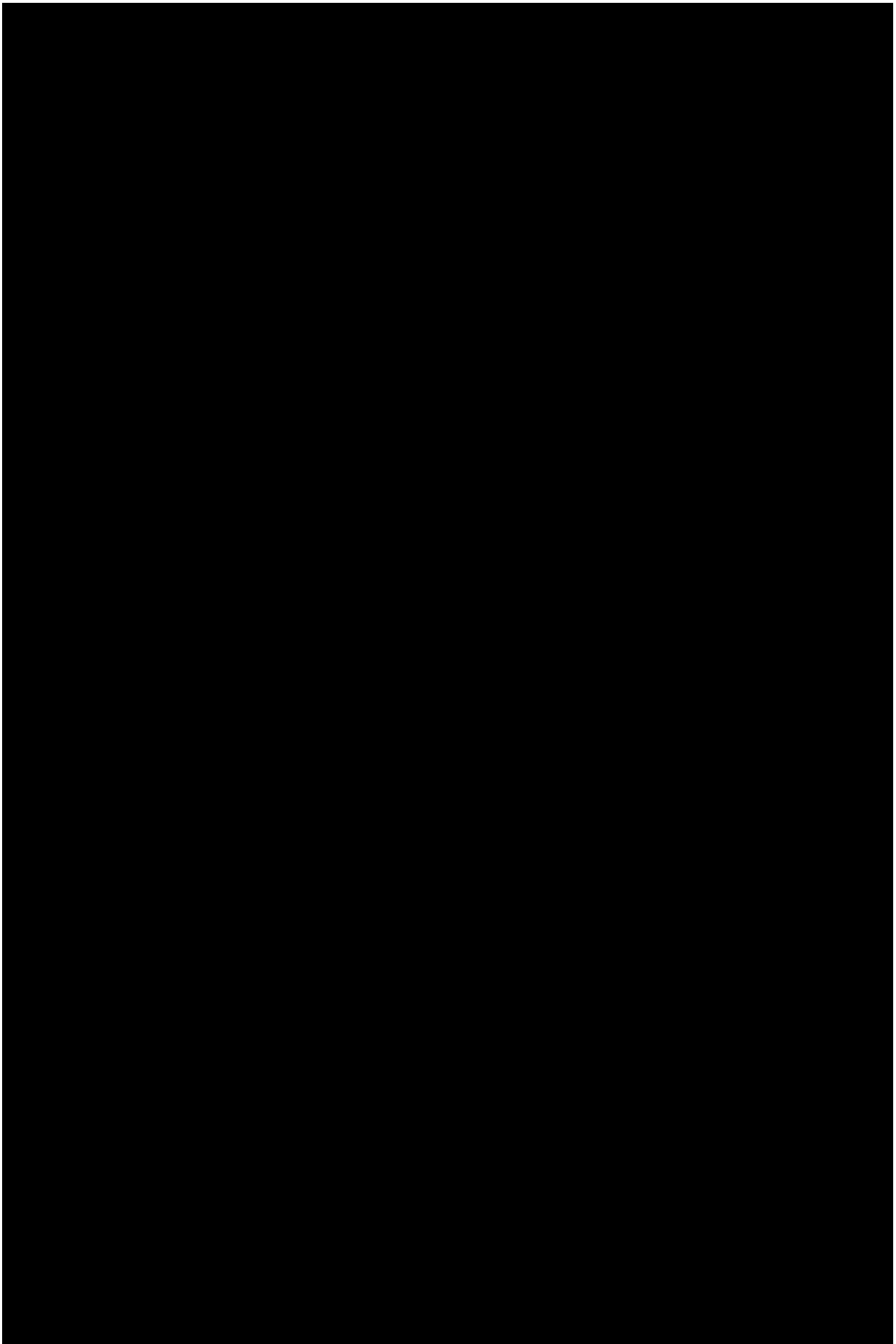


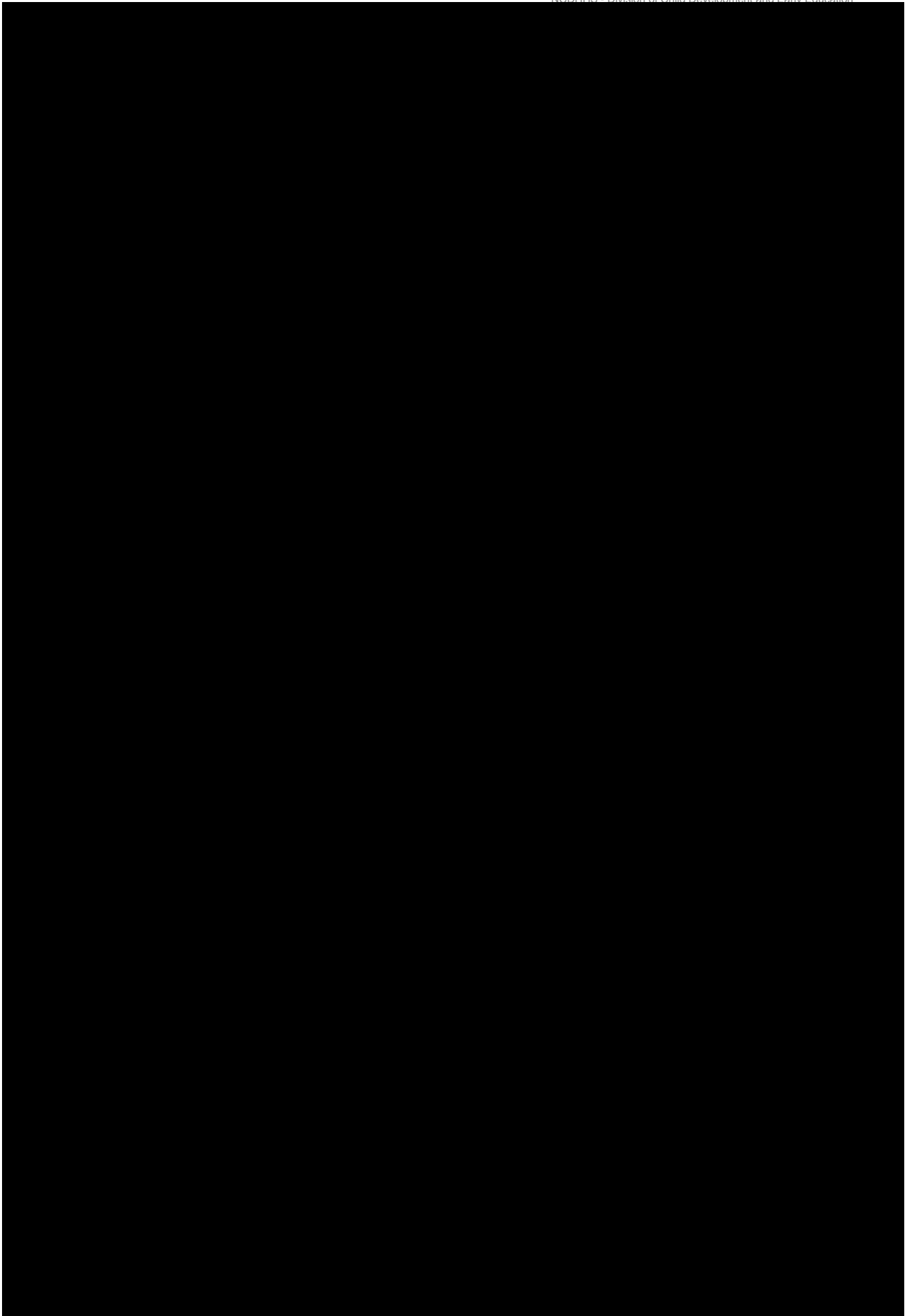


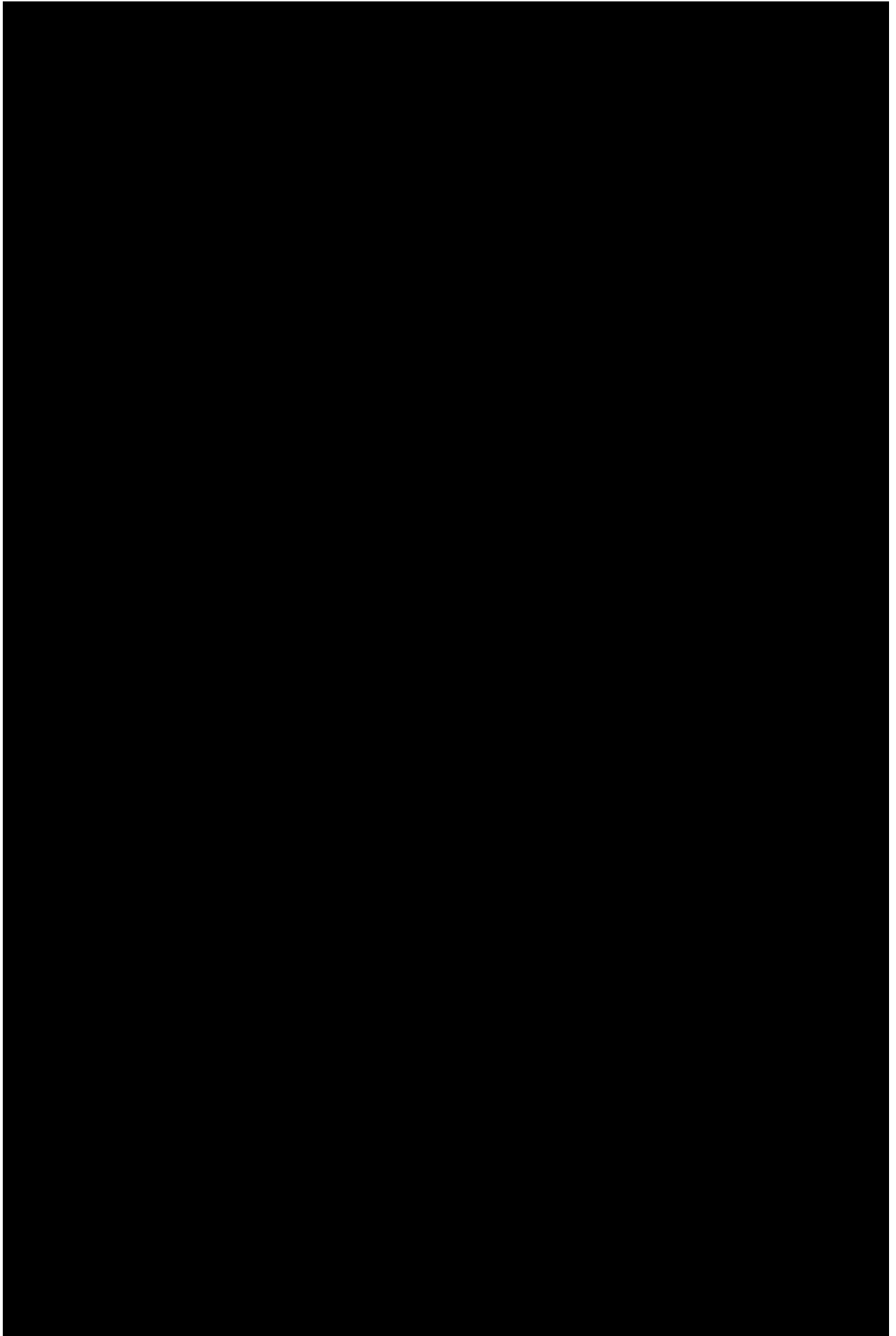


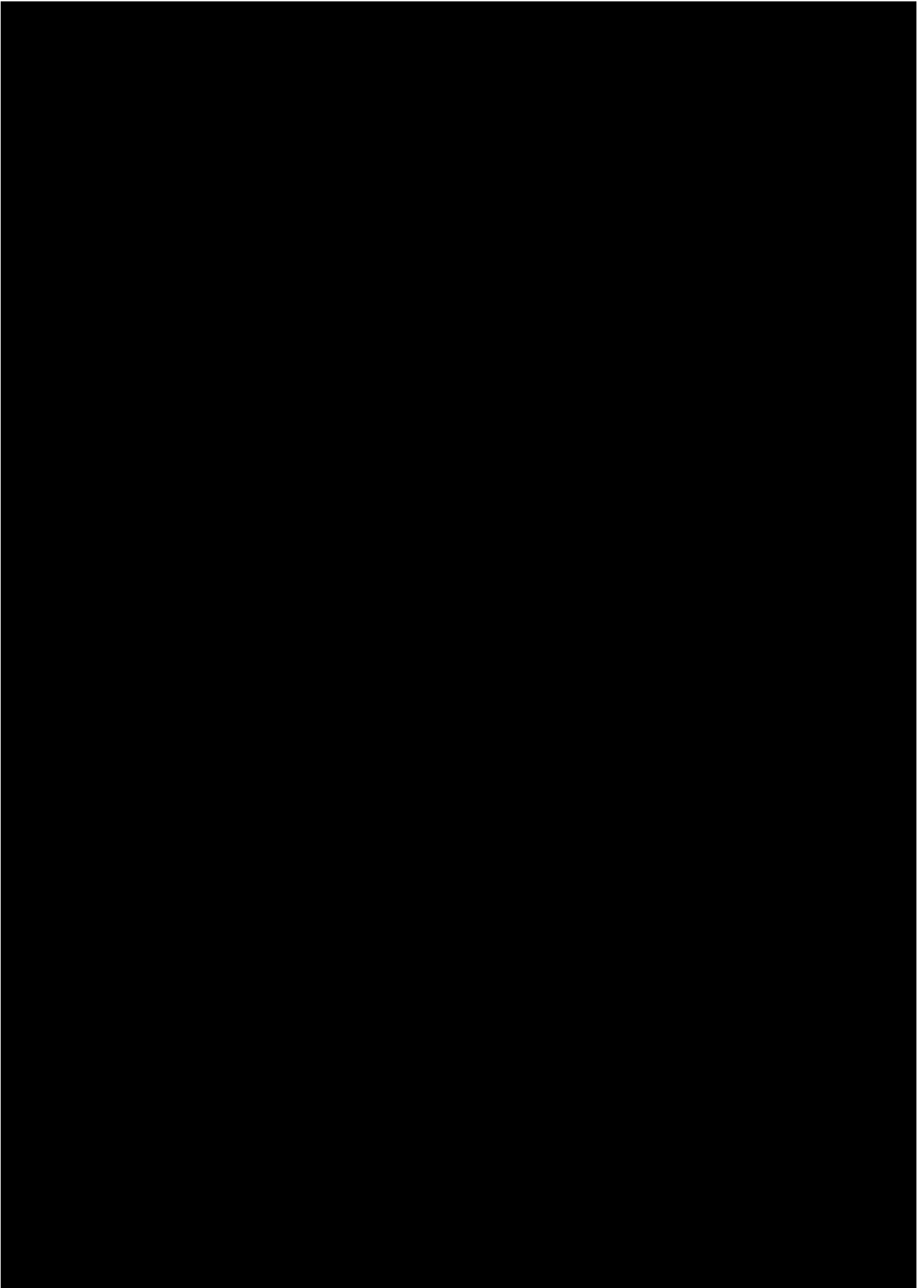


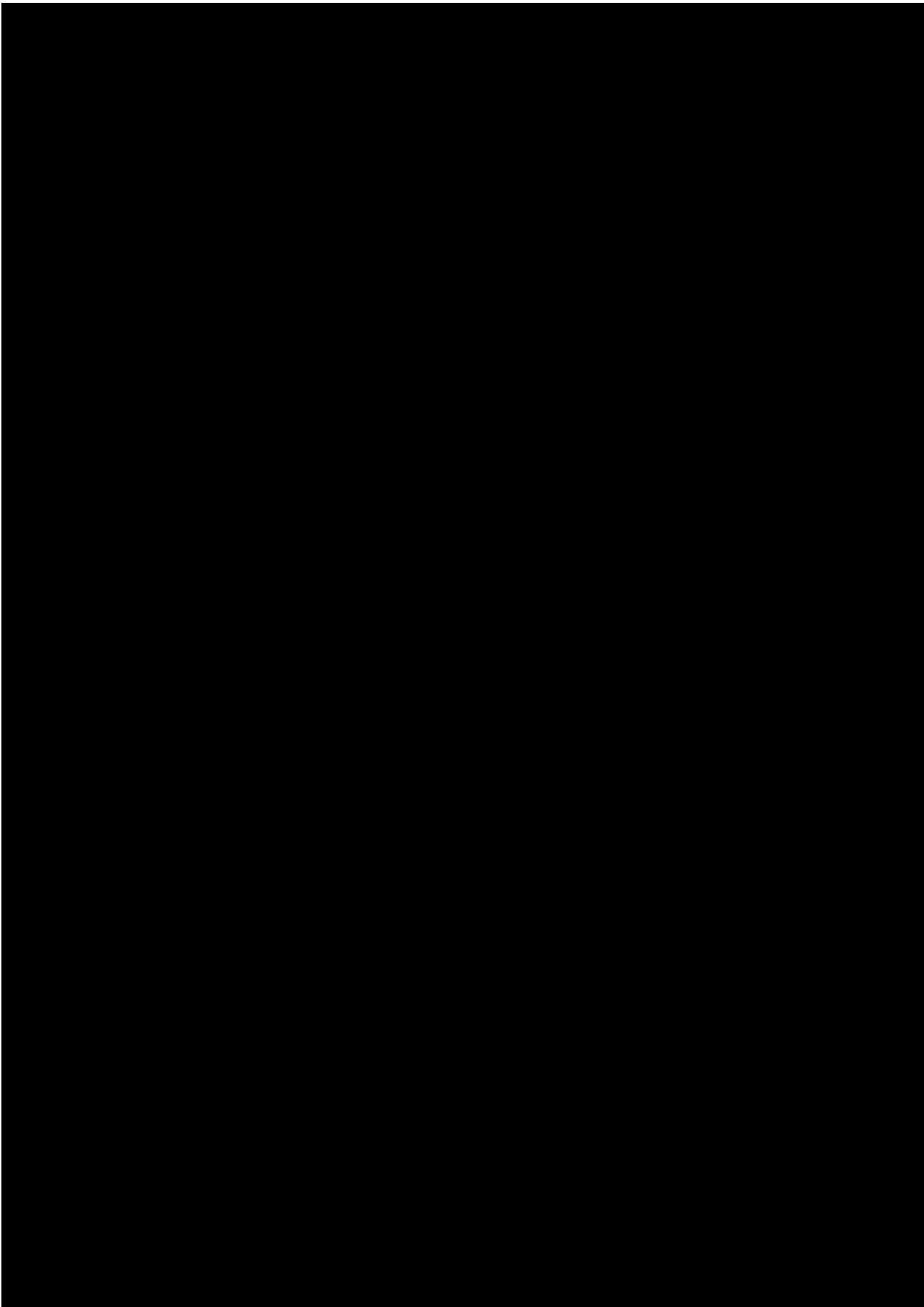


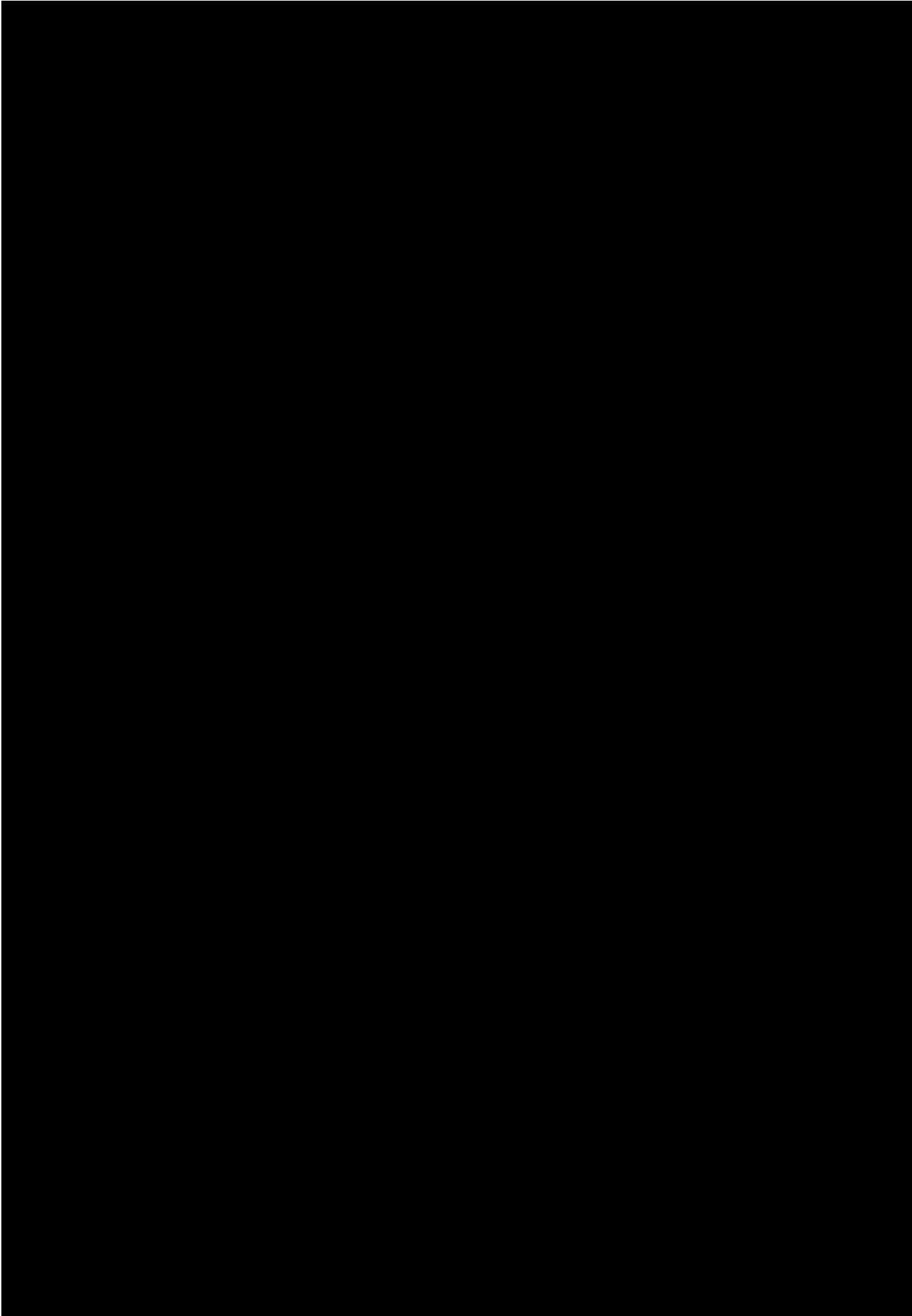


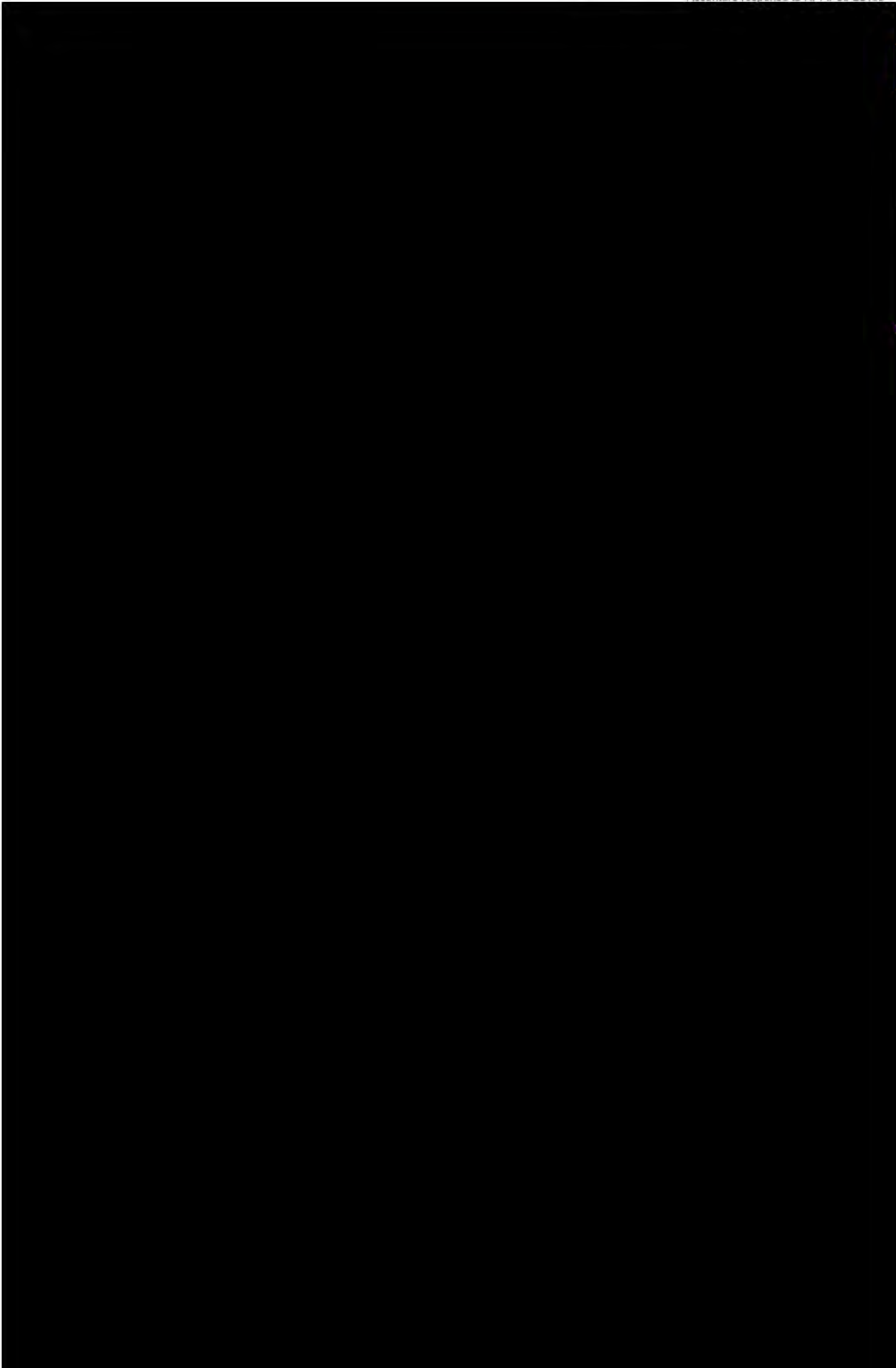


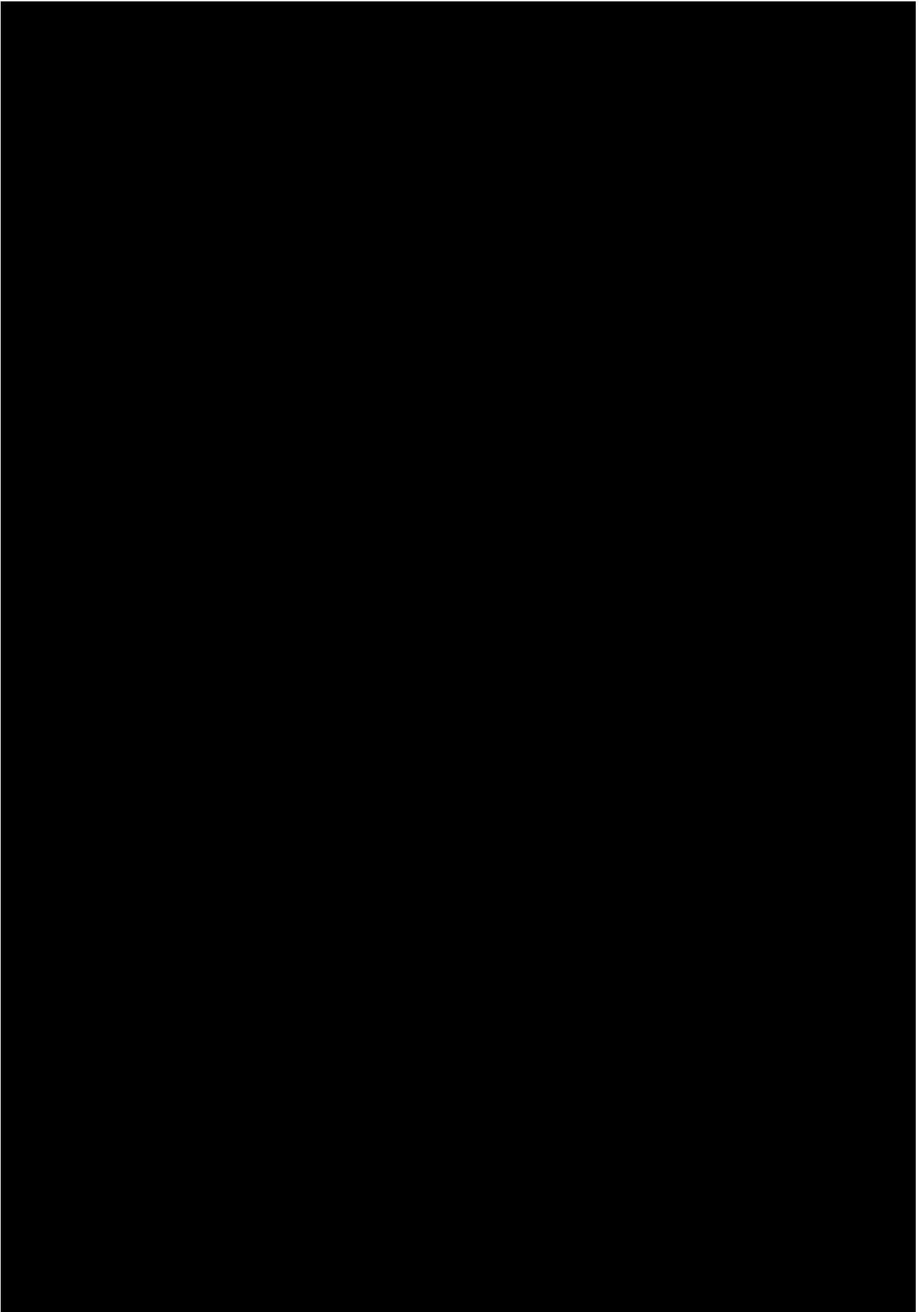


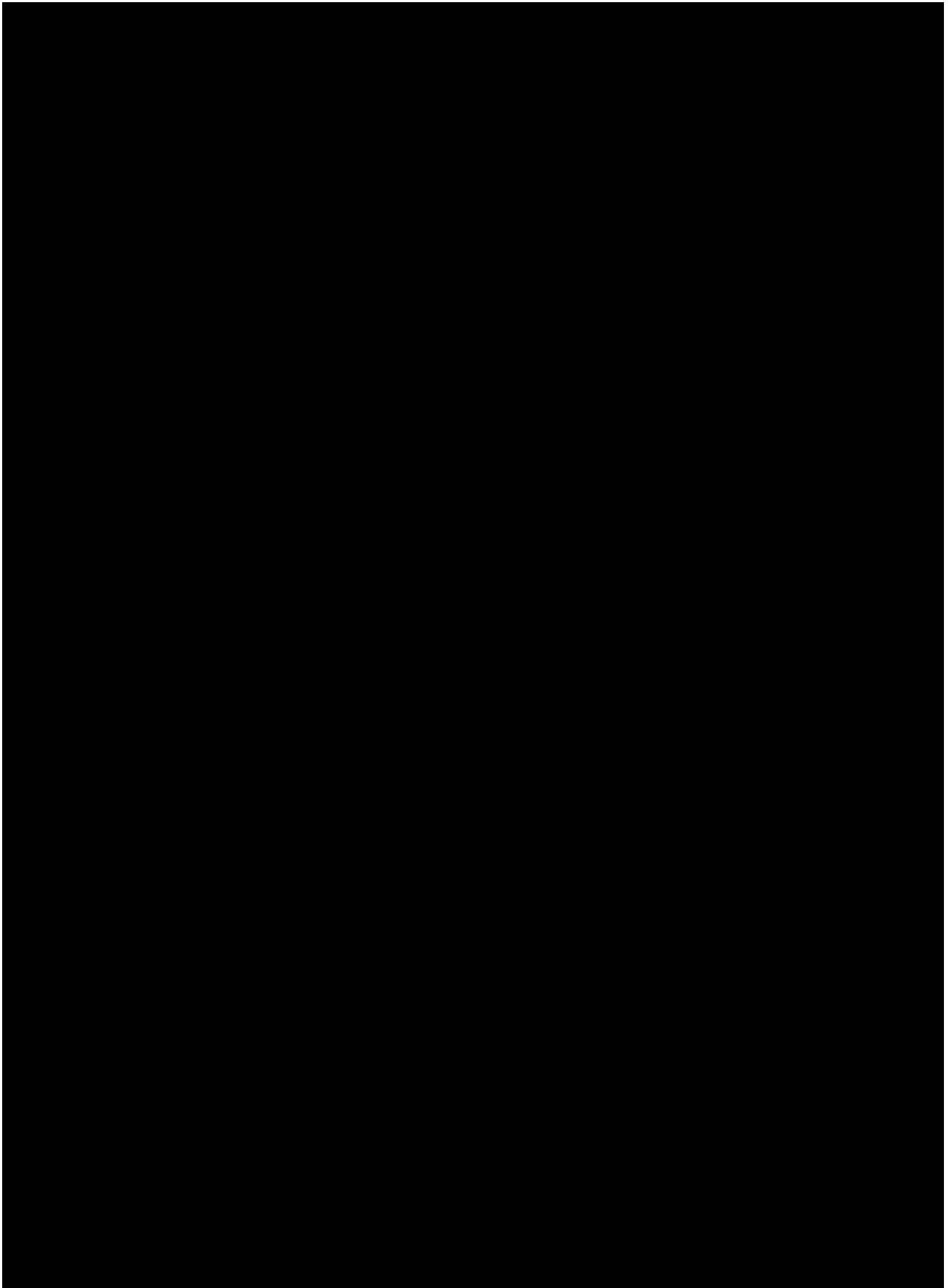


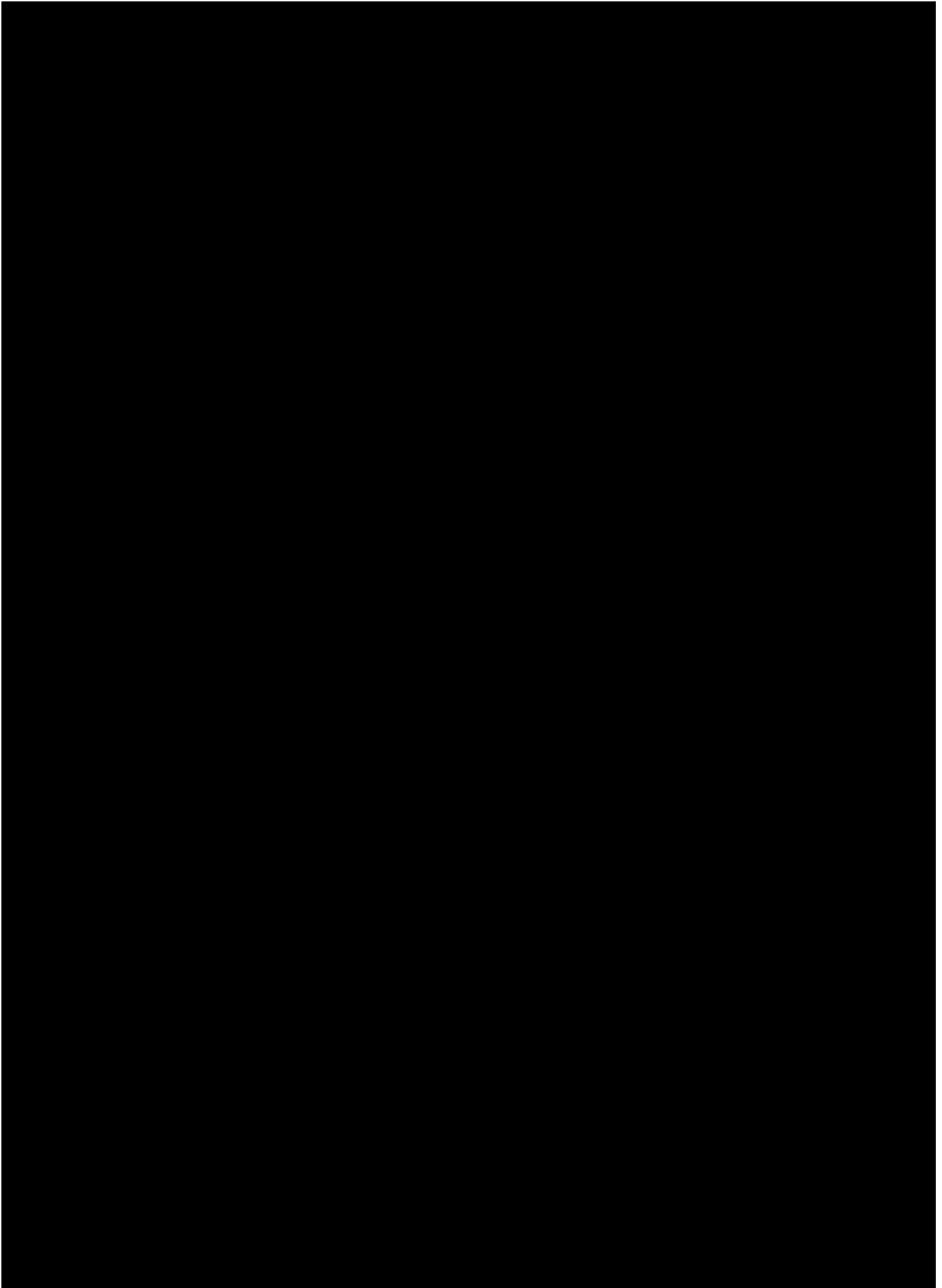


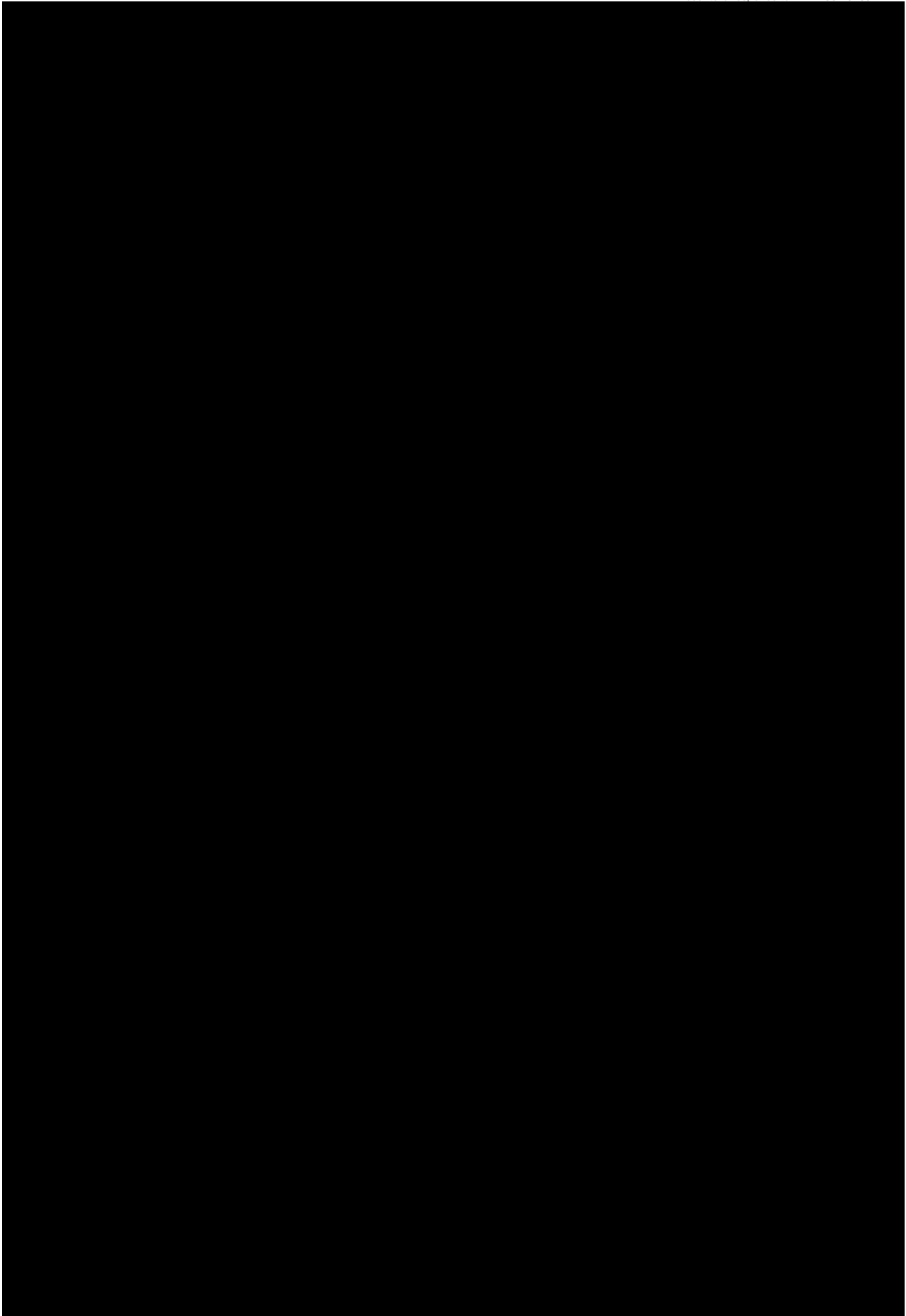


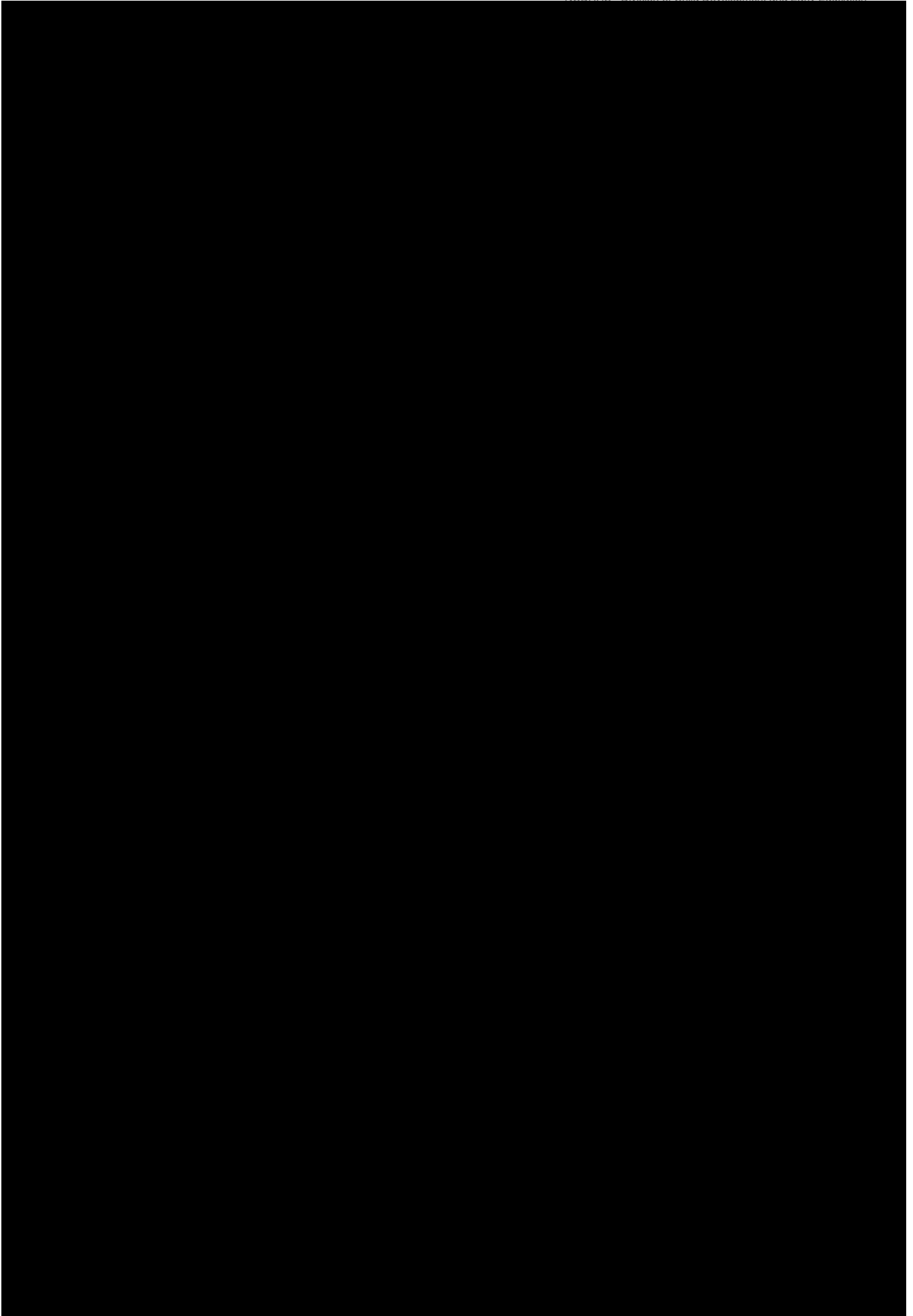


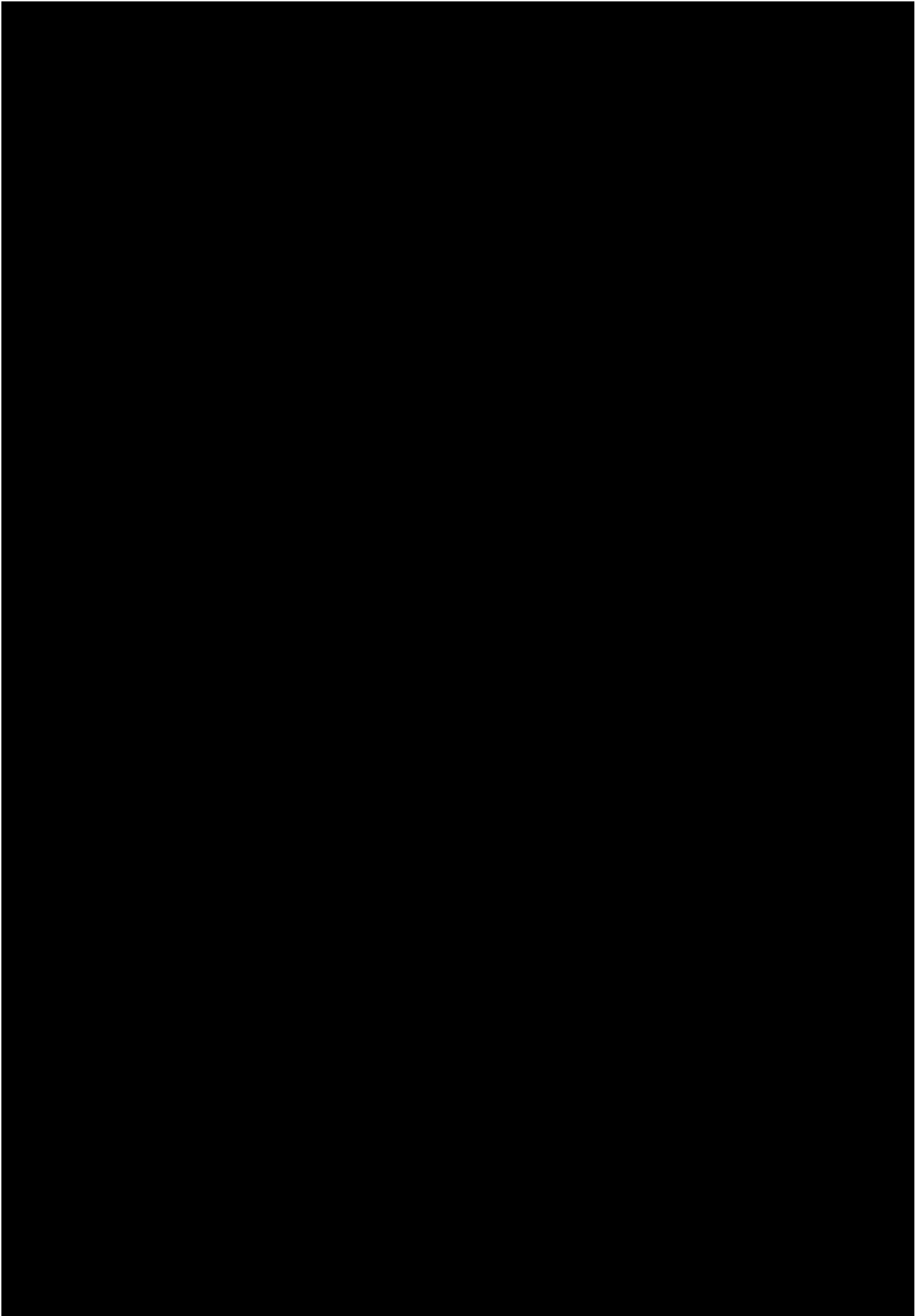


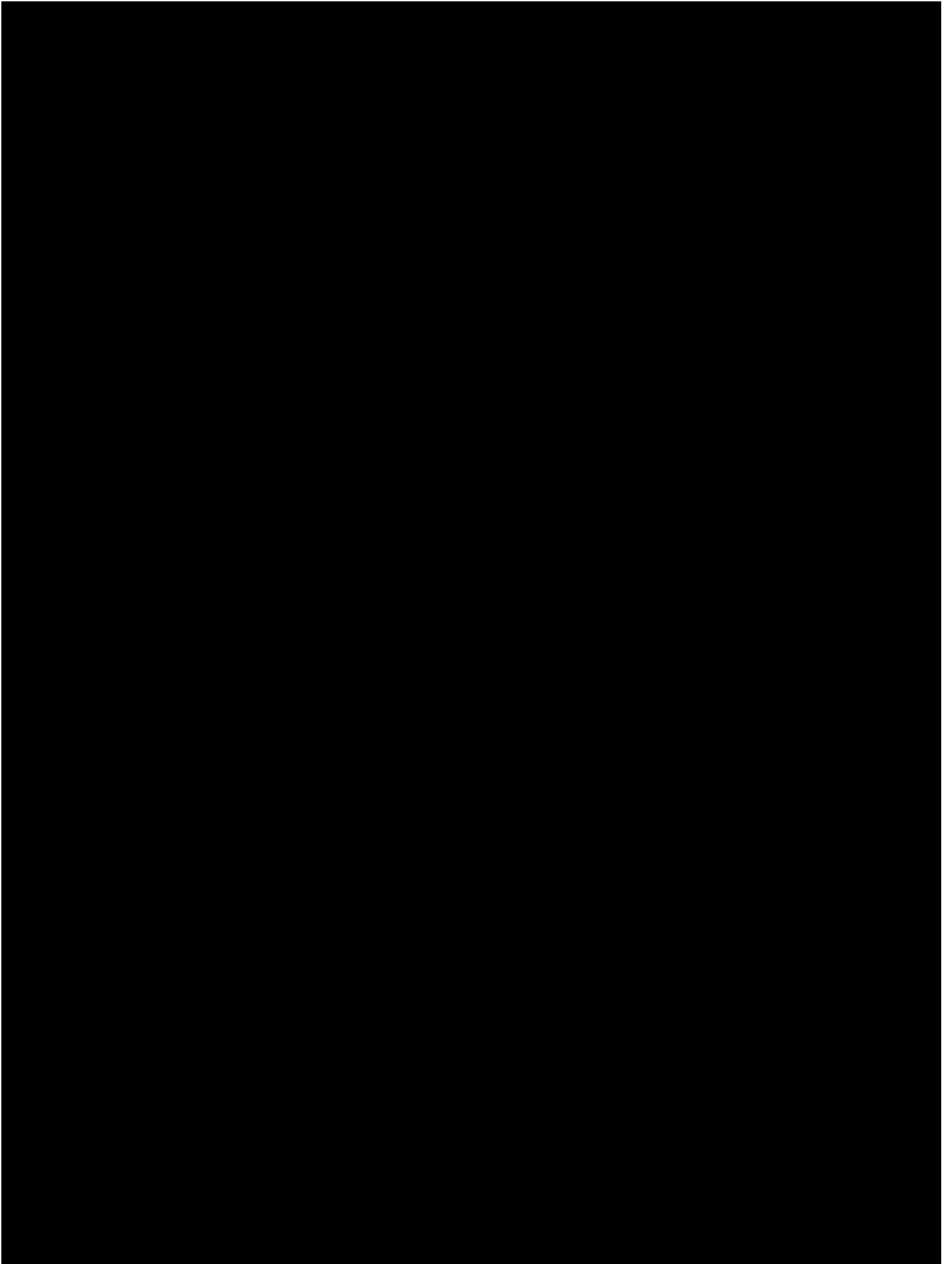


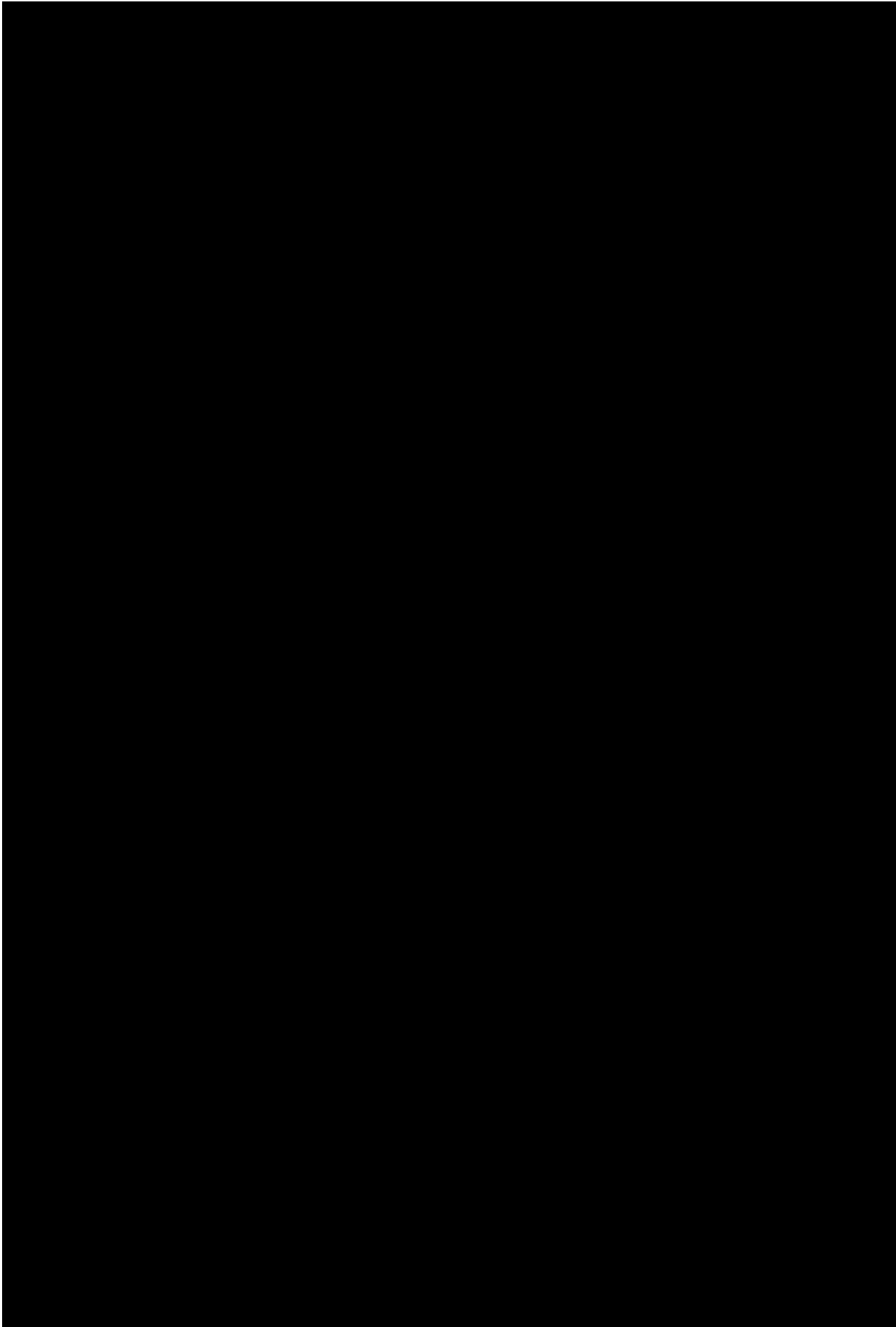


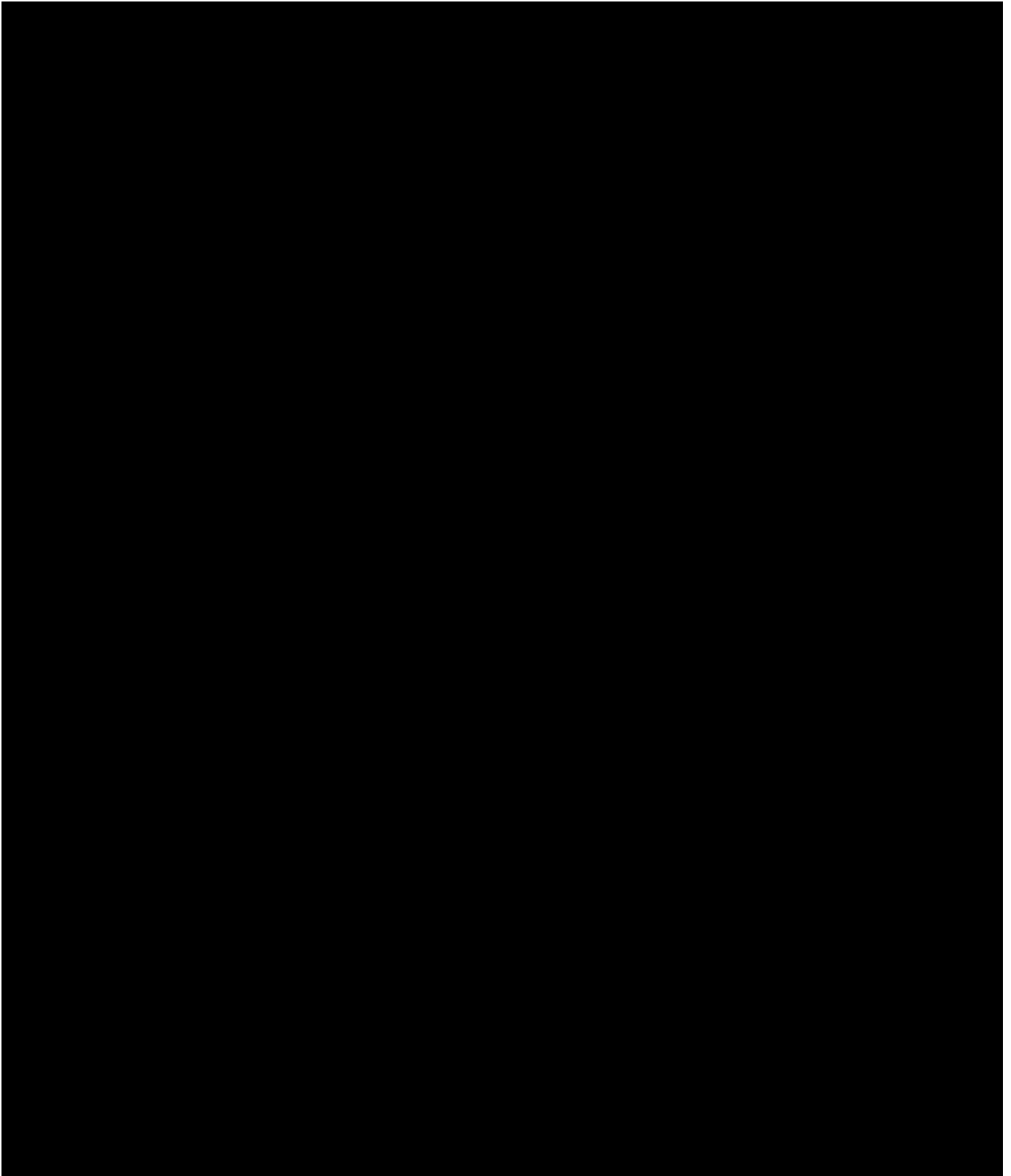


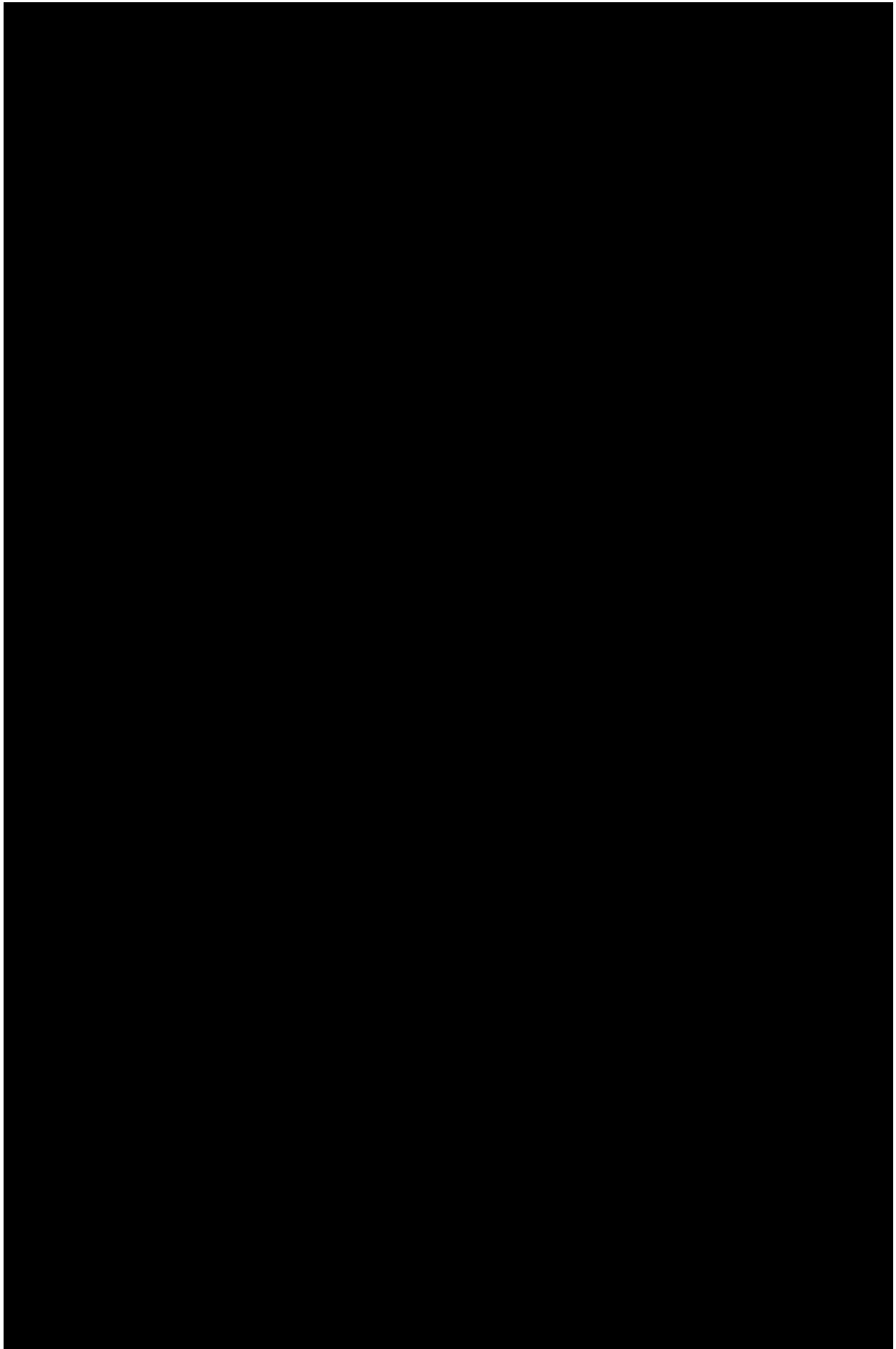


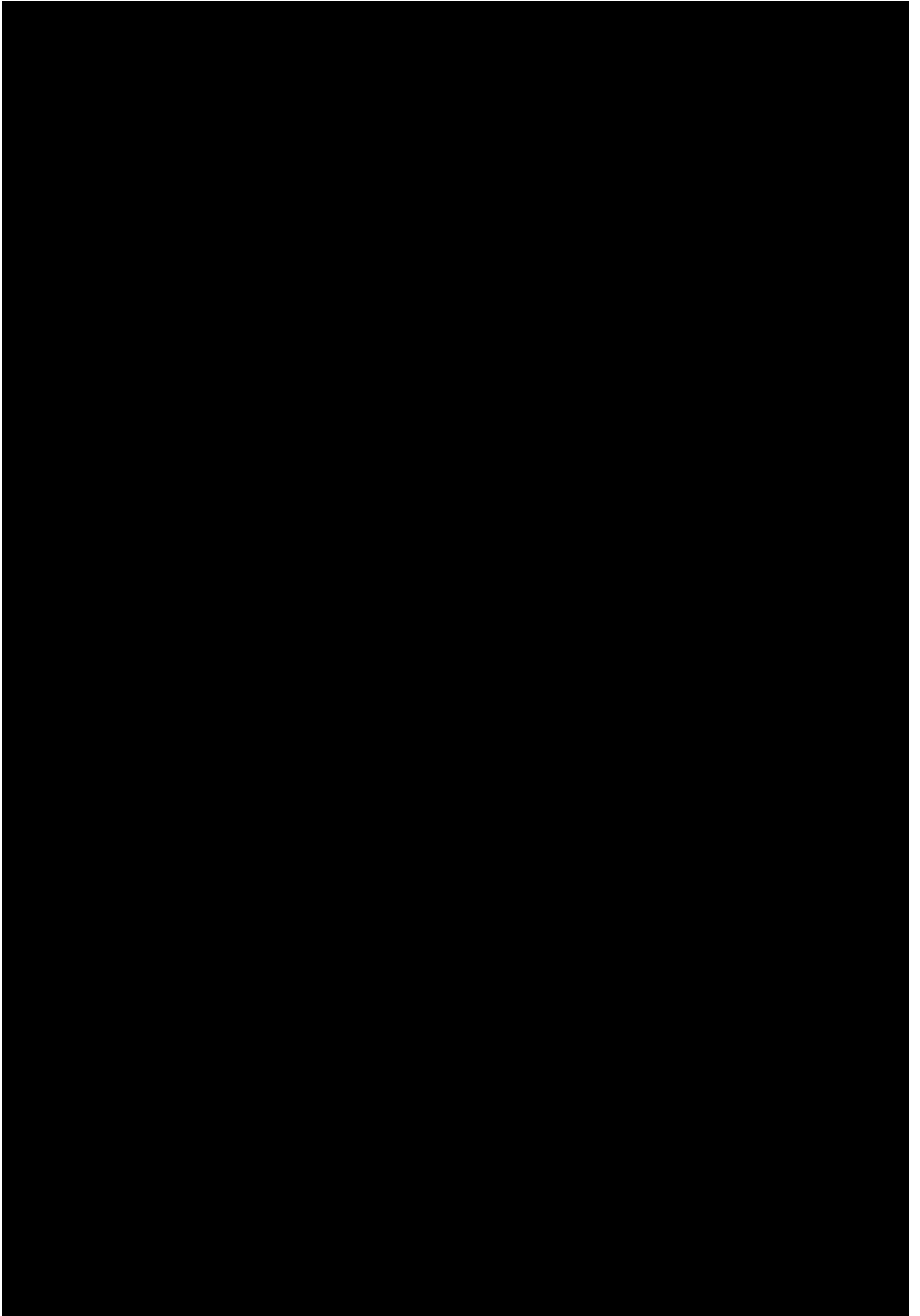


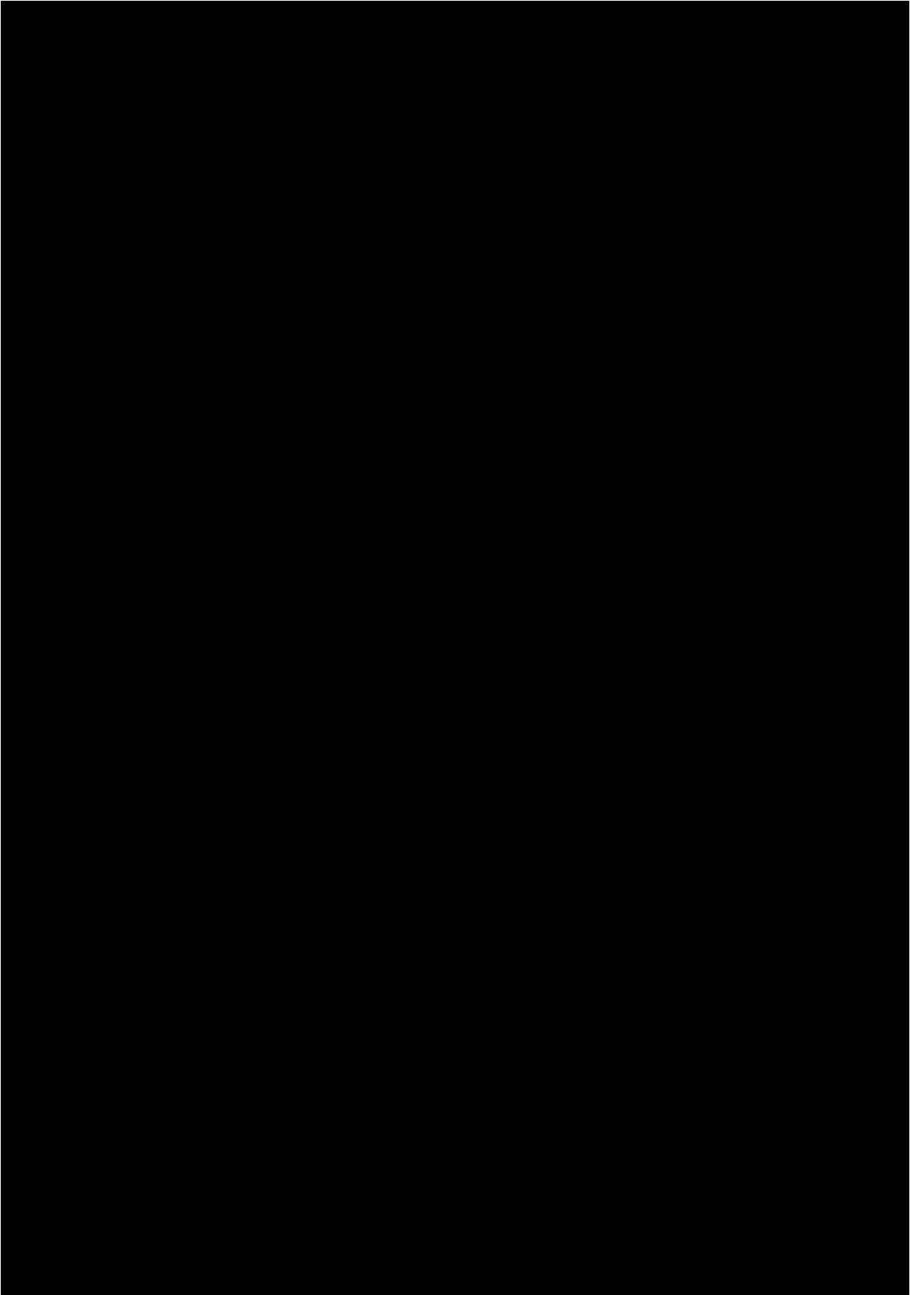










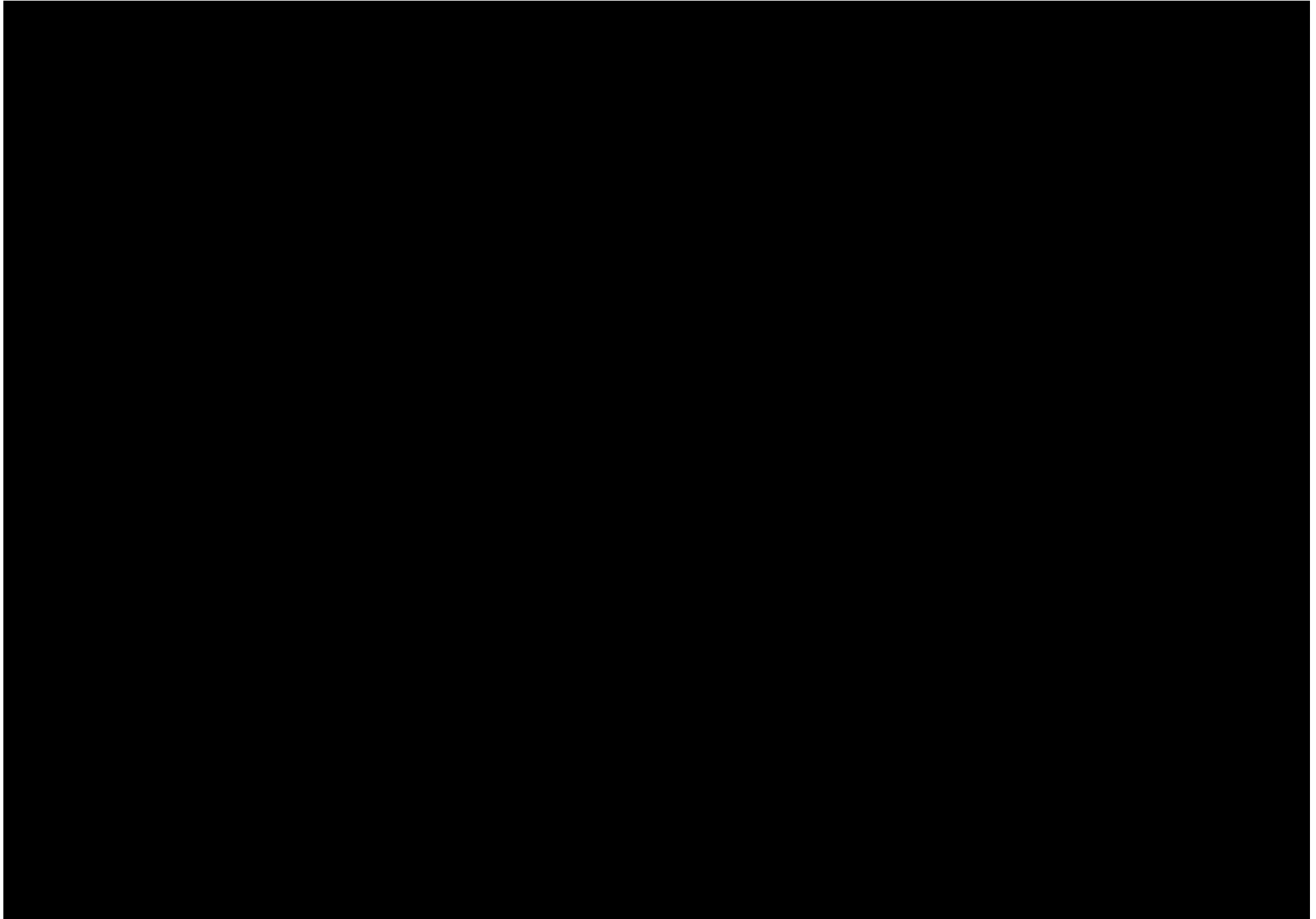


2.0 Draft Vendor Project Schedule

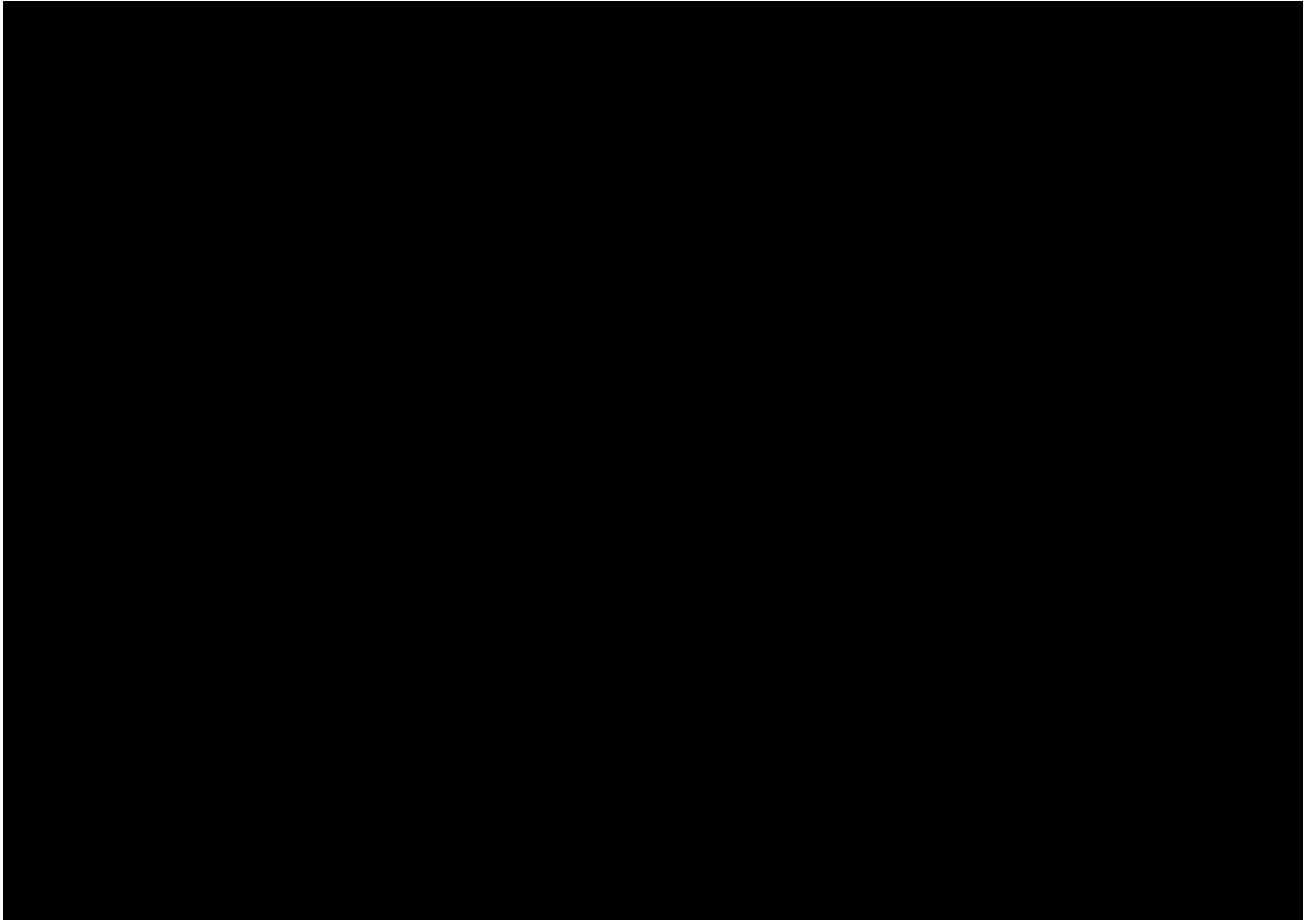
Vendor Project Schedule will: be developed with Microsoft Project™ or a Microsoft Project compatible product. Minimum Content:

- Clearly map to the State's and NCDHHS's Project Management Stages, and Sprint cycles /Modules /Milestones and Deliverables outlined in this RFP;
 - Sub-divide all tasks until no more than eighty (80) hours are allocated to each task;
 - Identify each Sprint Cycles/Modules/Milestones/ Deliverables cycle
 - Identify capability/functionality developed by the Sprint Cycles/Modules/Milestones/ Deliverables
 - The expected duration of the Sprint Cycles/Modules/Milestones/ Deliverables
 - The order of the Sprint Cycles/Modules/Milestones/ Deliverables
 - Projected task start and end dates;
 - Major business decision points and Deliverables defined in this RFP;
 - Projected Sprint Cycles/Modules/Milestones/decision point due dates;
 - Task dependencies;
 - WBS references for each task and Sprint Cycles/Modules/Milestones;
 - Resource task assignments and usage for all NC NCDHHS staff, Vendor staff, and project team staff from any other organizations; and
 - When allocating work to Agency or other State personnel, the Vendor Project Schedule must:
 - o Be based upon a forty-hour (40) week (8:00 a.m. through 5:00 p.m., Monday through Friday Eastern Time); and
 - o Accommodate that many of the Agency or other State personnel will not be assigned full time to this project and will not complete work on North Carolina State Government holidays (<https://oshr.nc.gov/state-employee-resources/benefits/leave/holidays>).
-

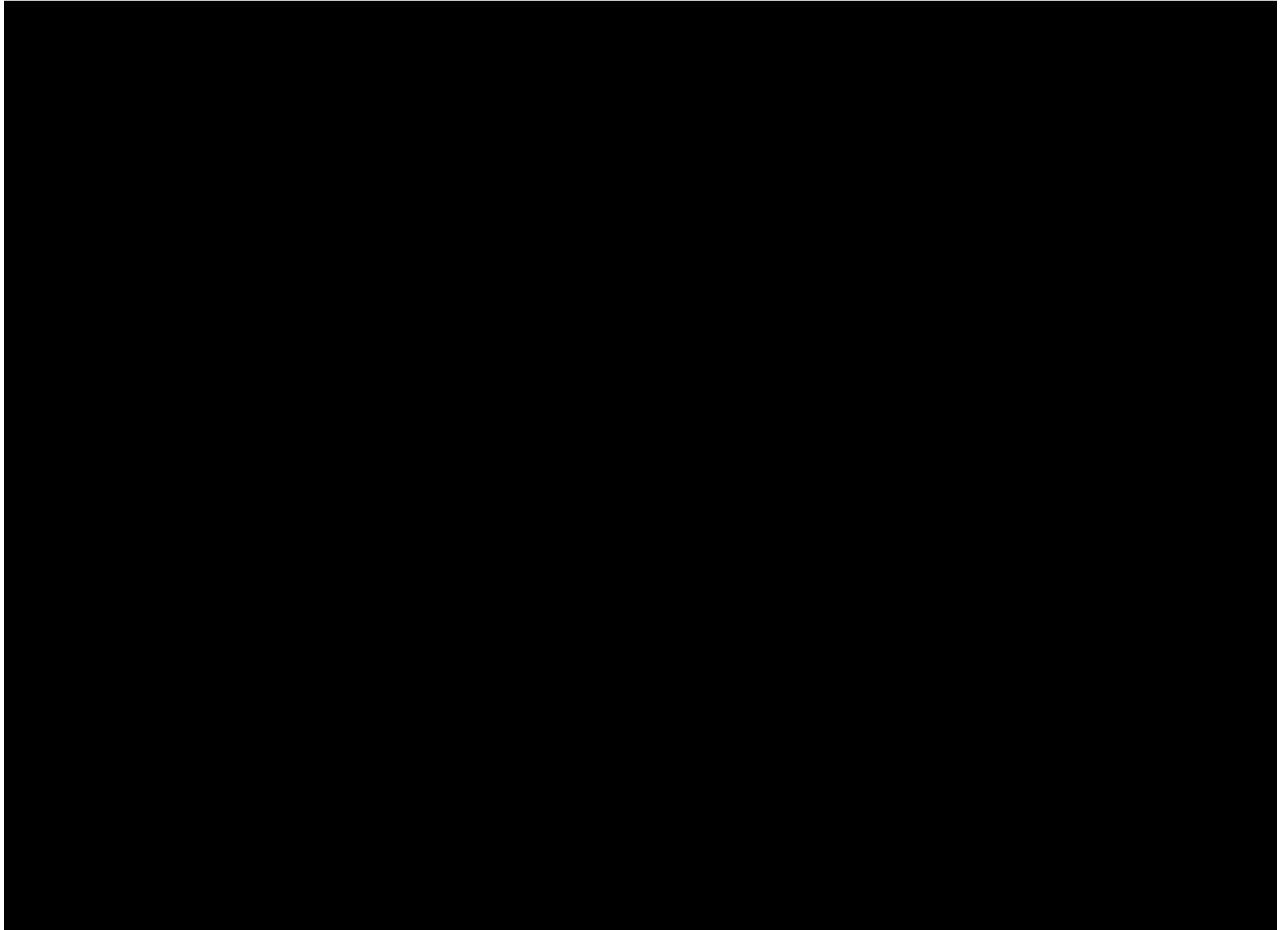
CONFIDENTIAL

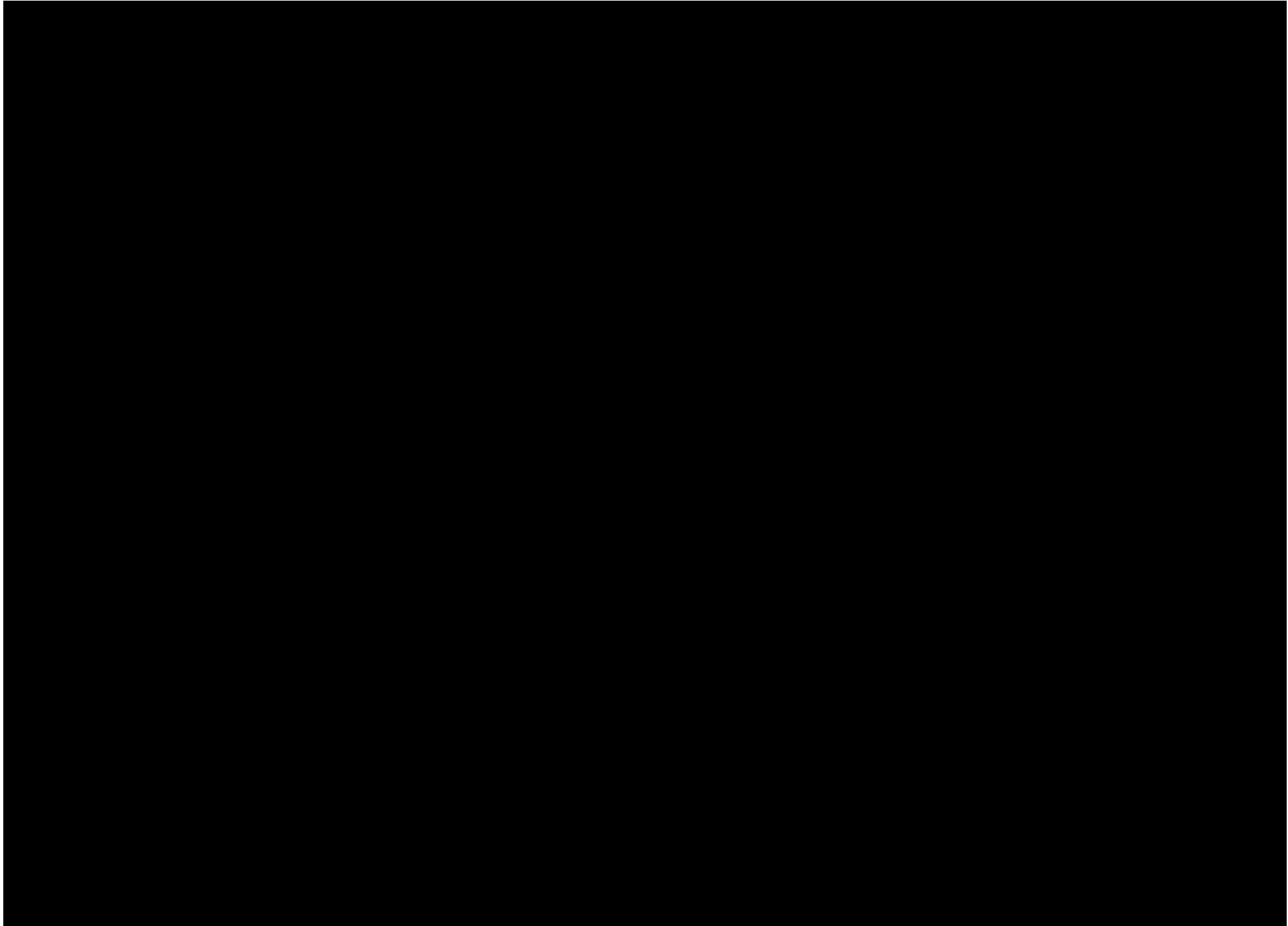


CONFIDENTIAL

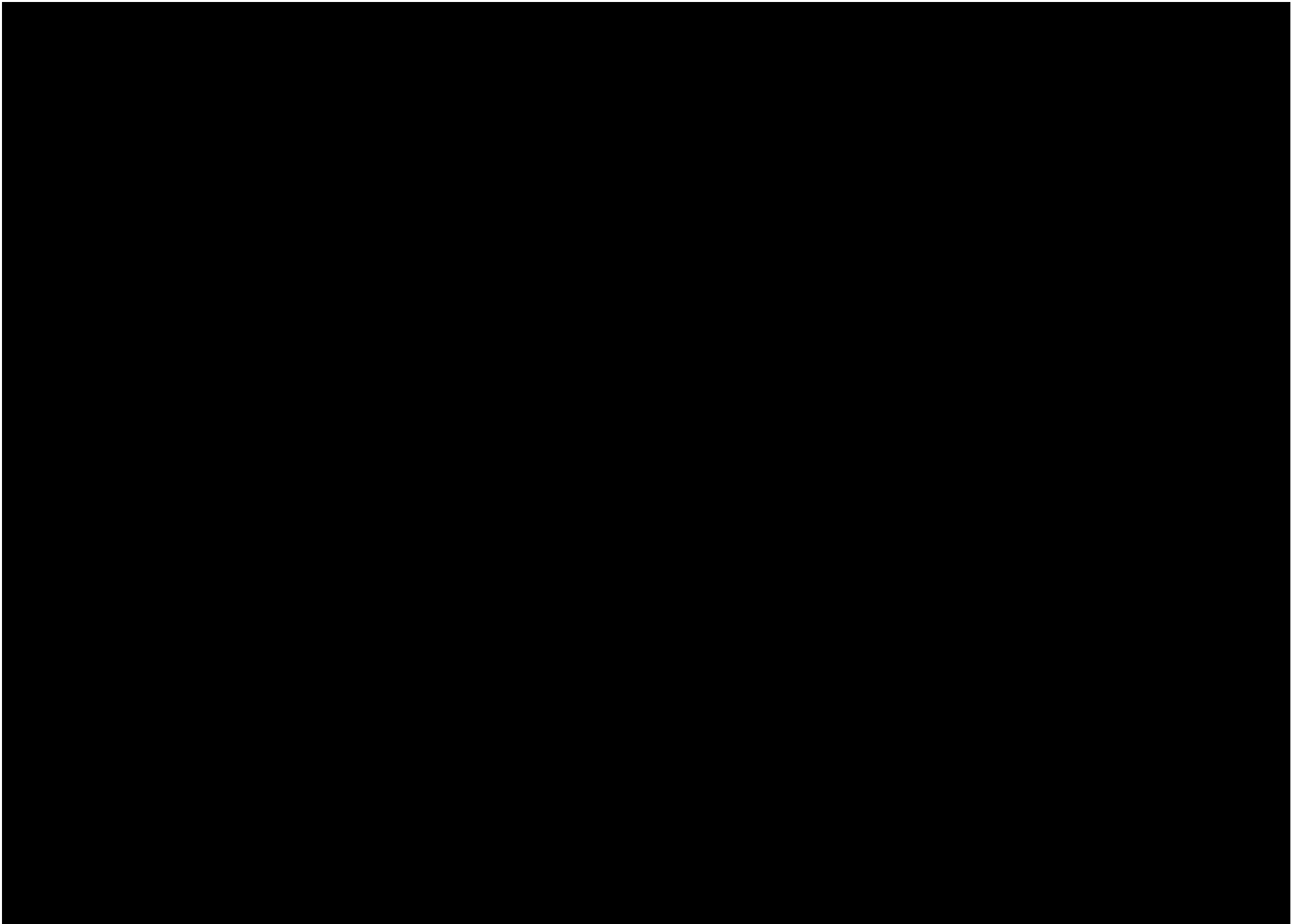


CONFIDENTIAL

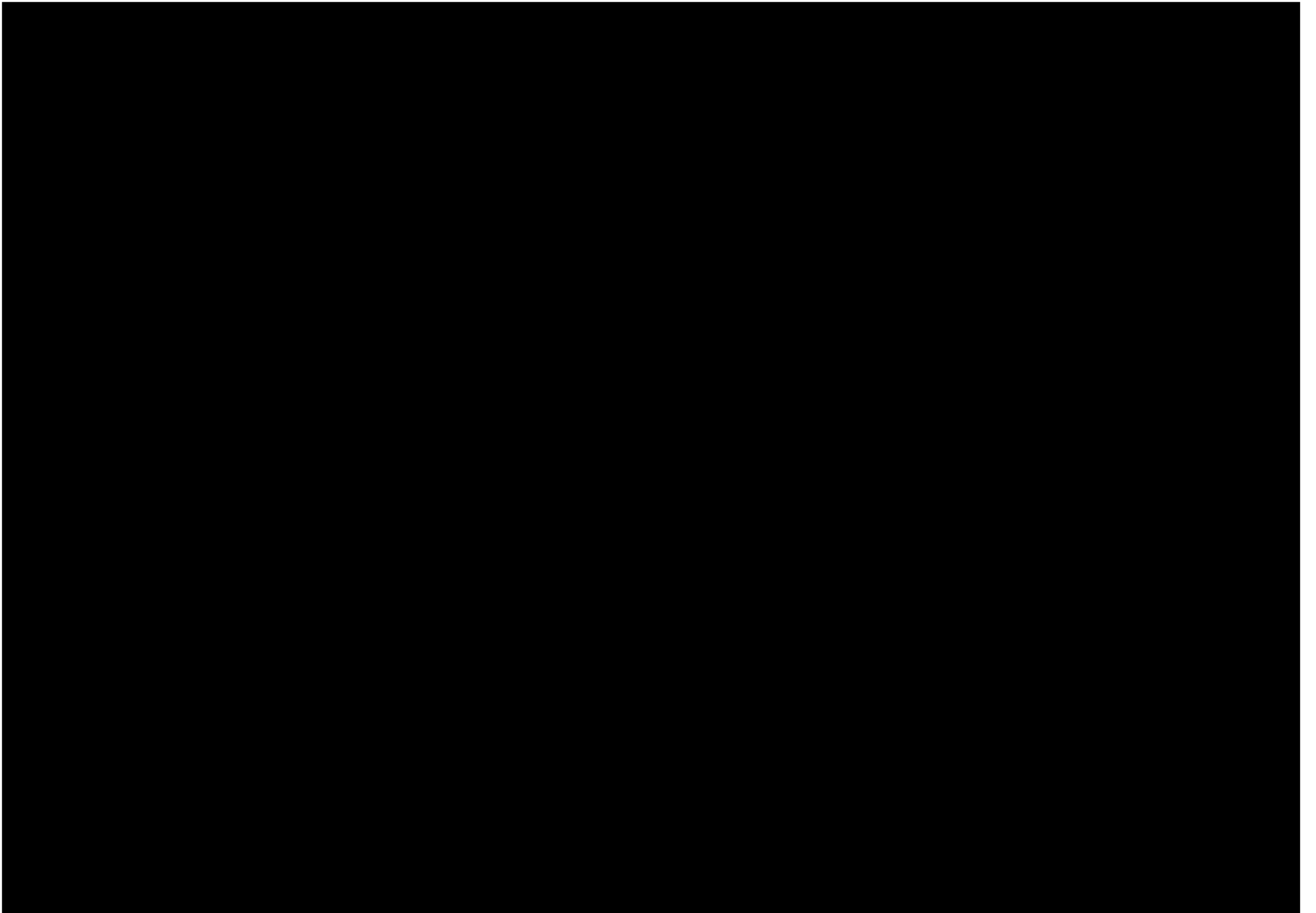




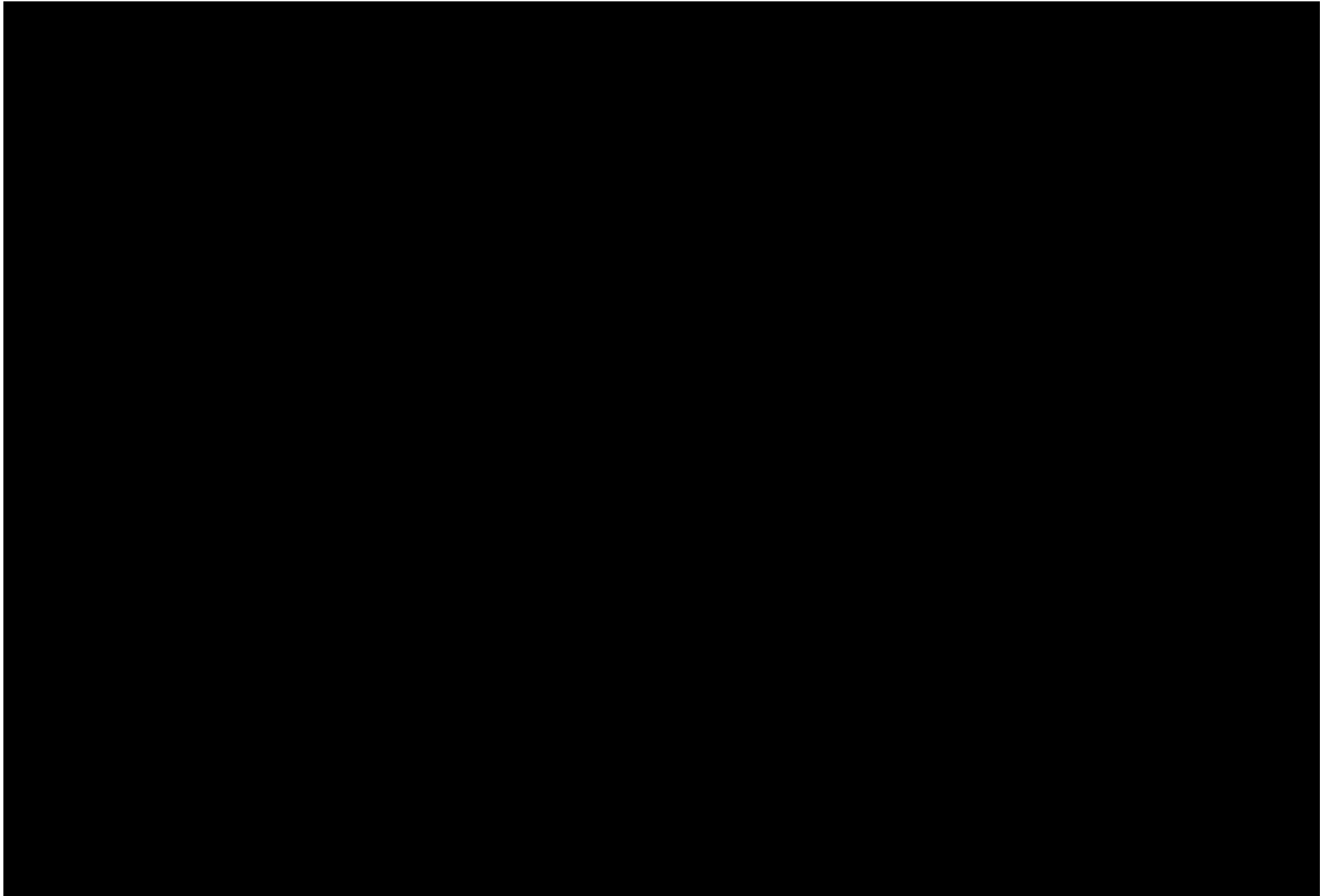
CONFIDENTIAL



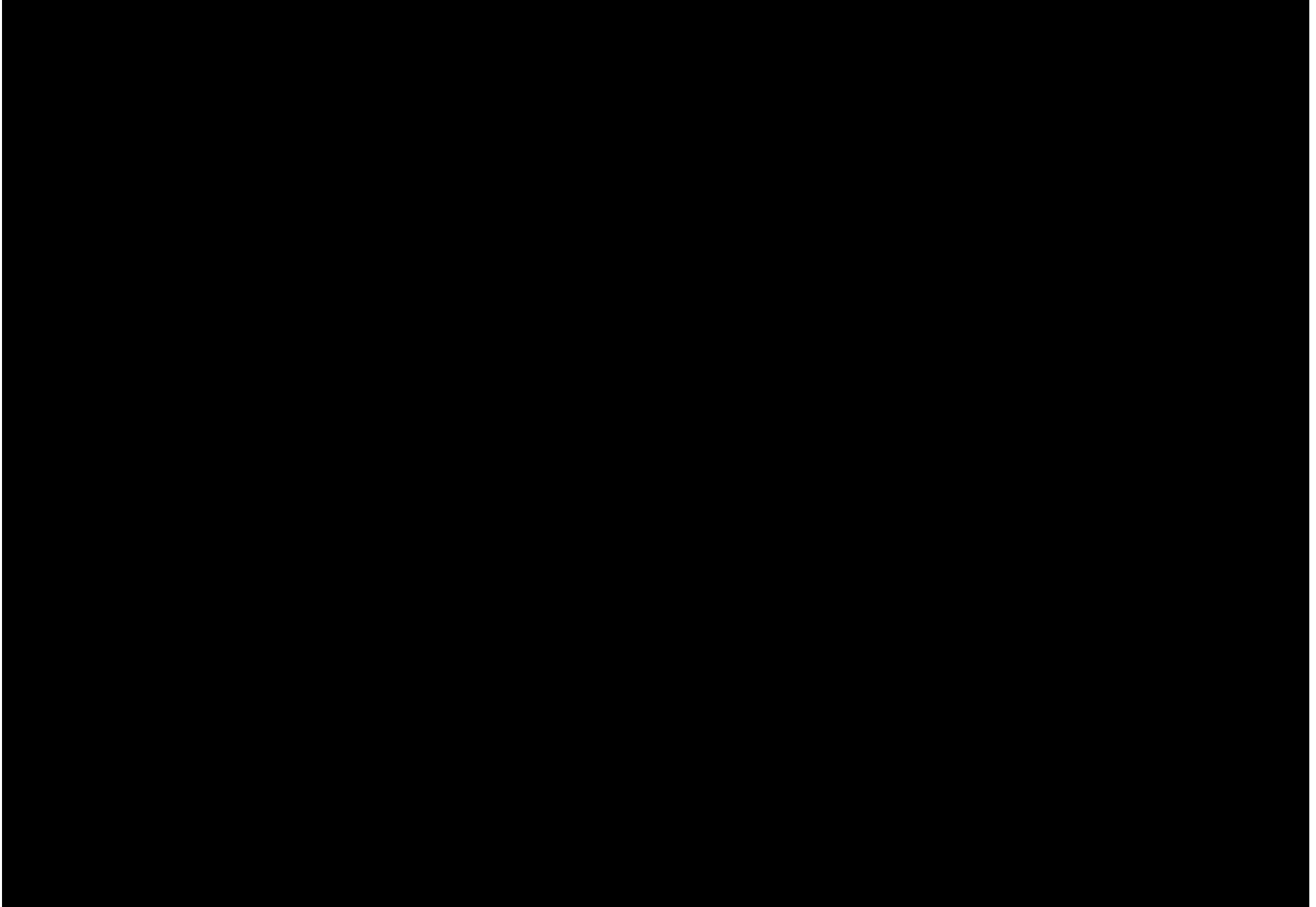
CONFIDENTIAL



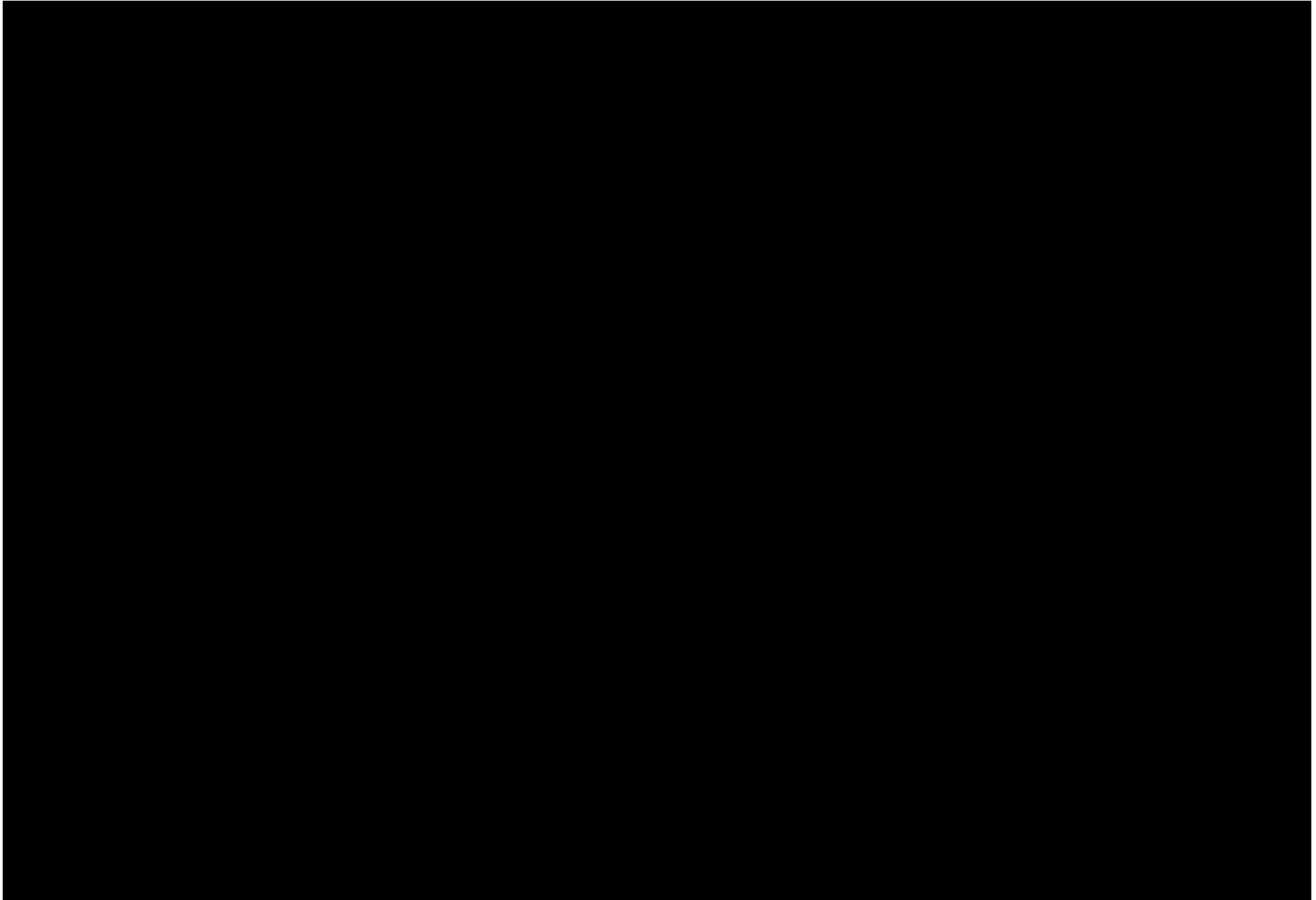
CONFIDENTIAL



CONFIDENTIAL

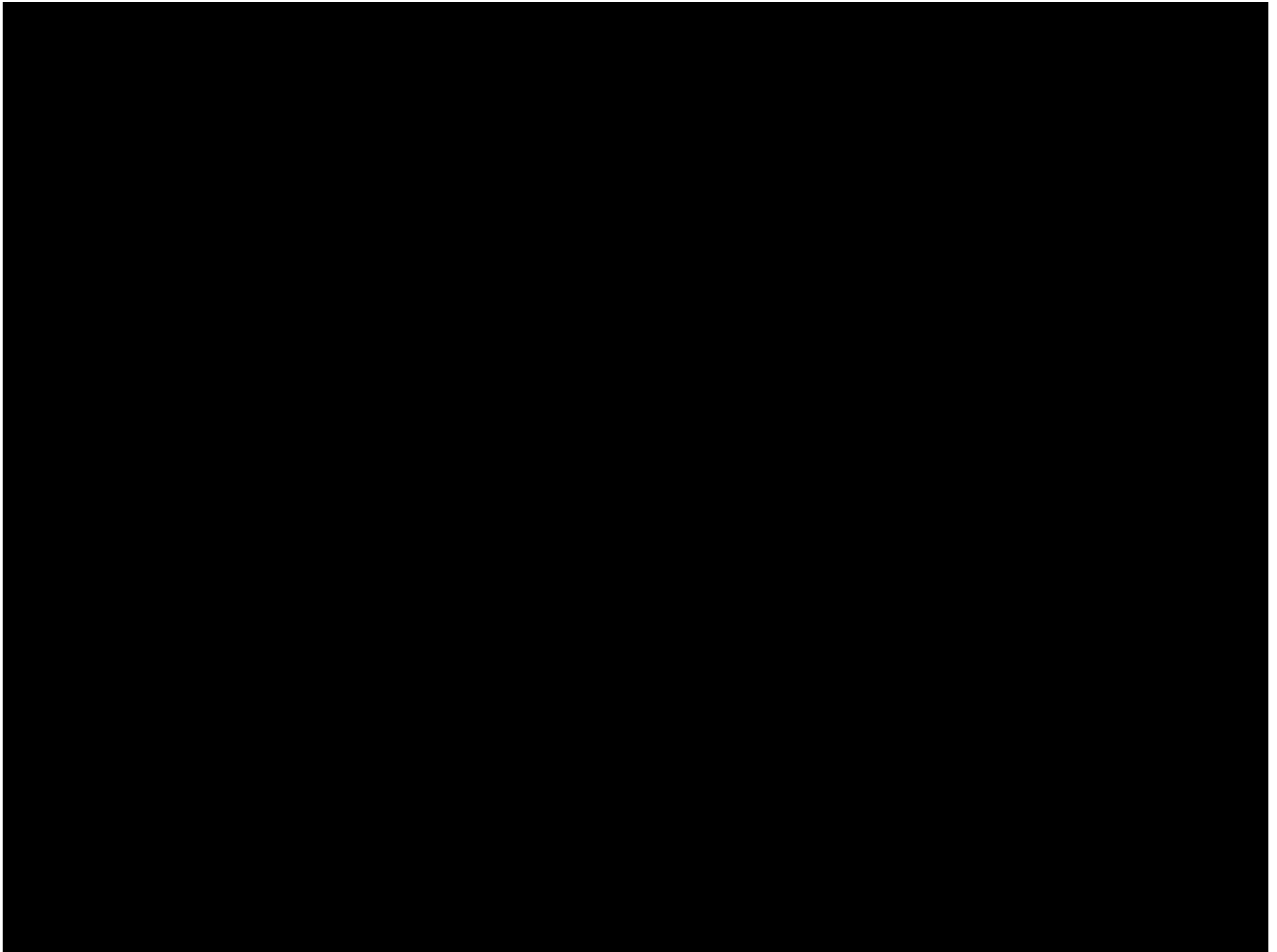


CONFIDENTIAL

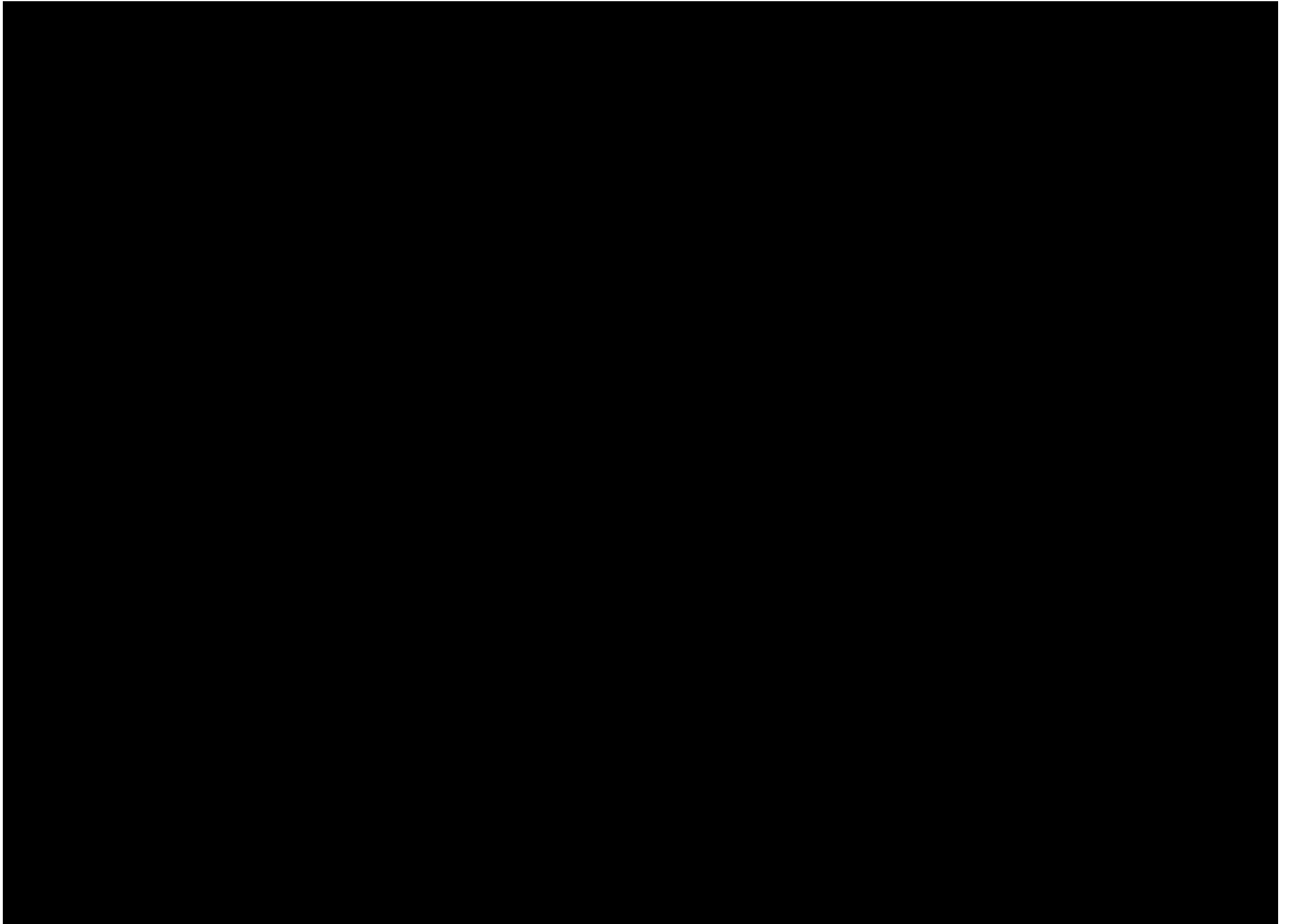


CONFIDENTIAL

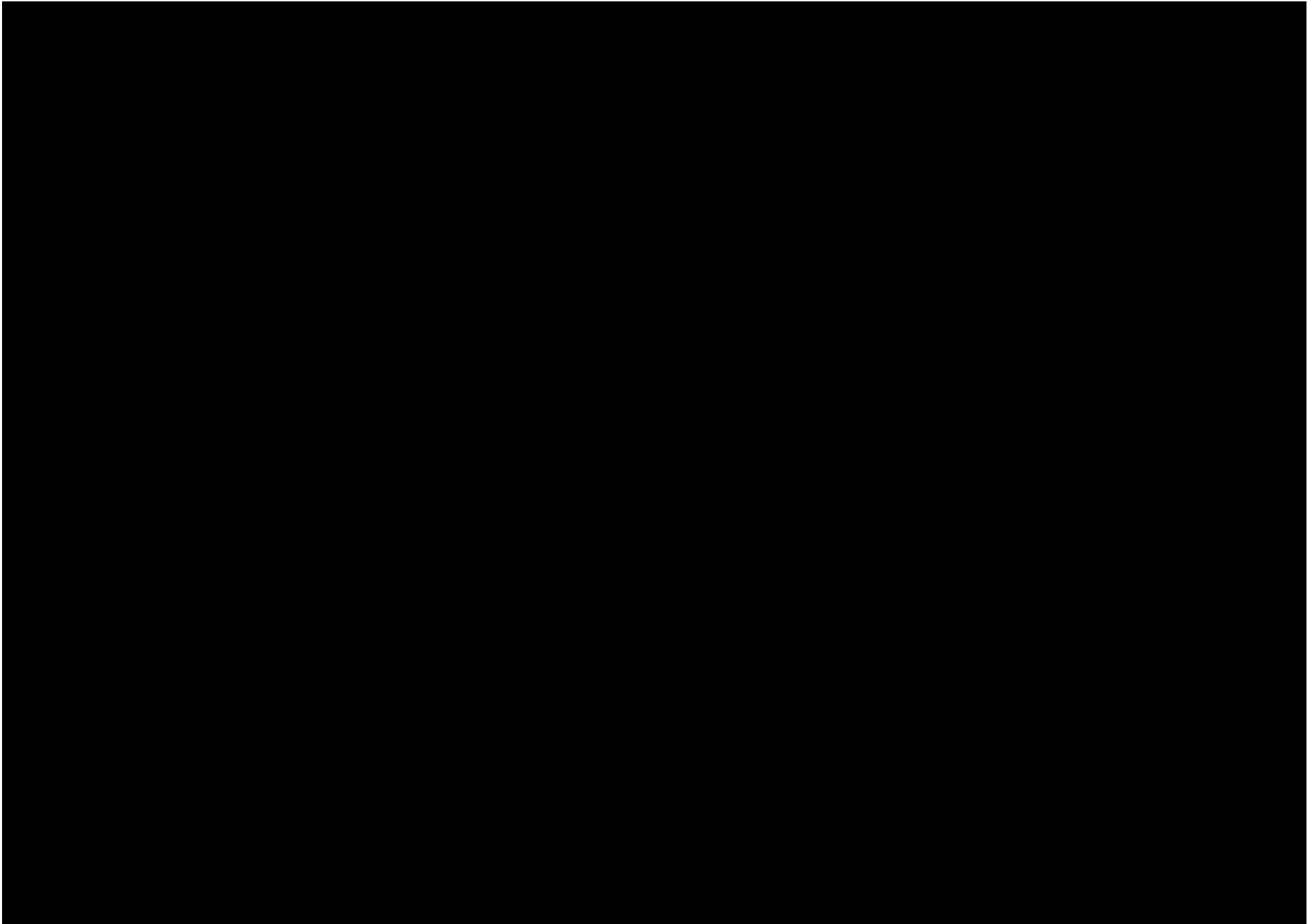
CONFIDENTIAL



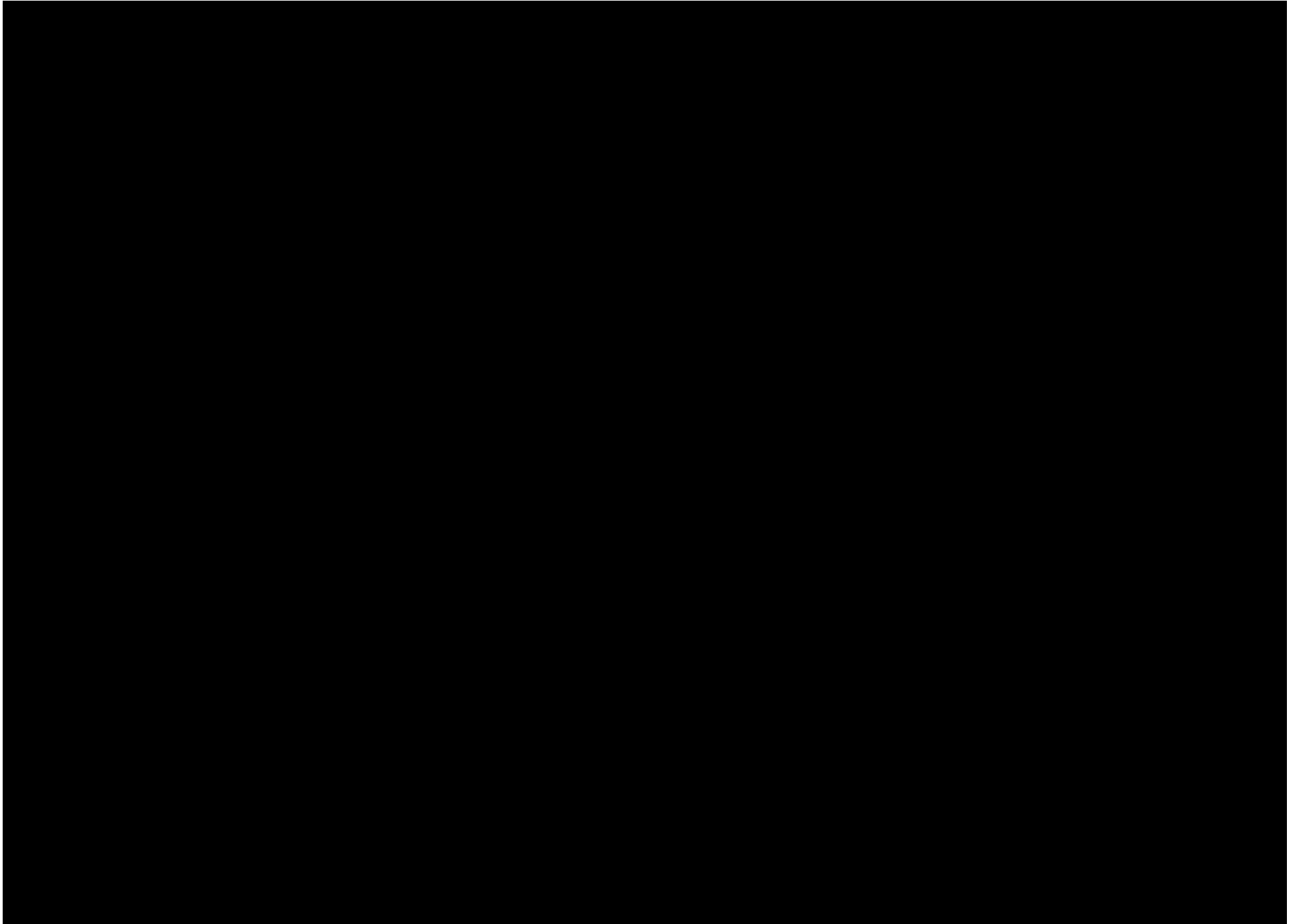
CONFIDENTIAL



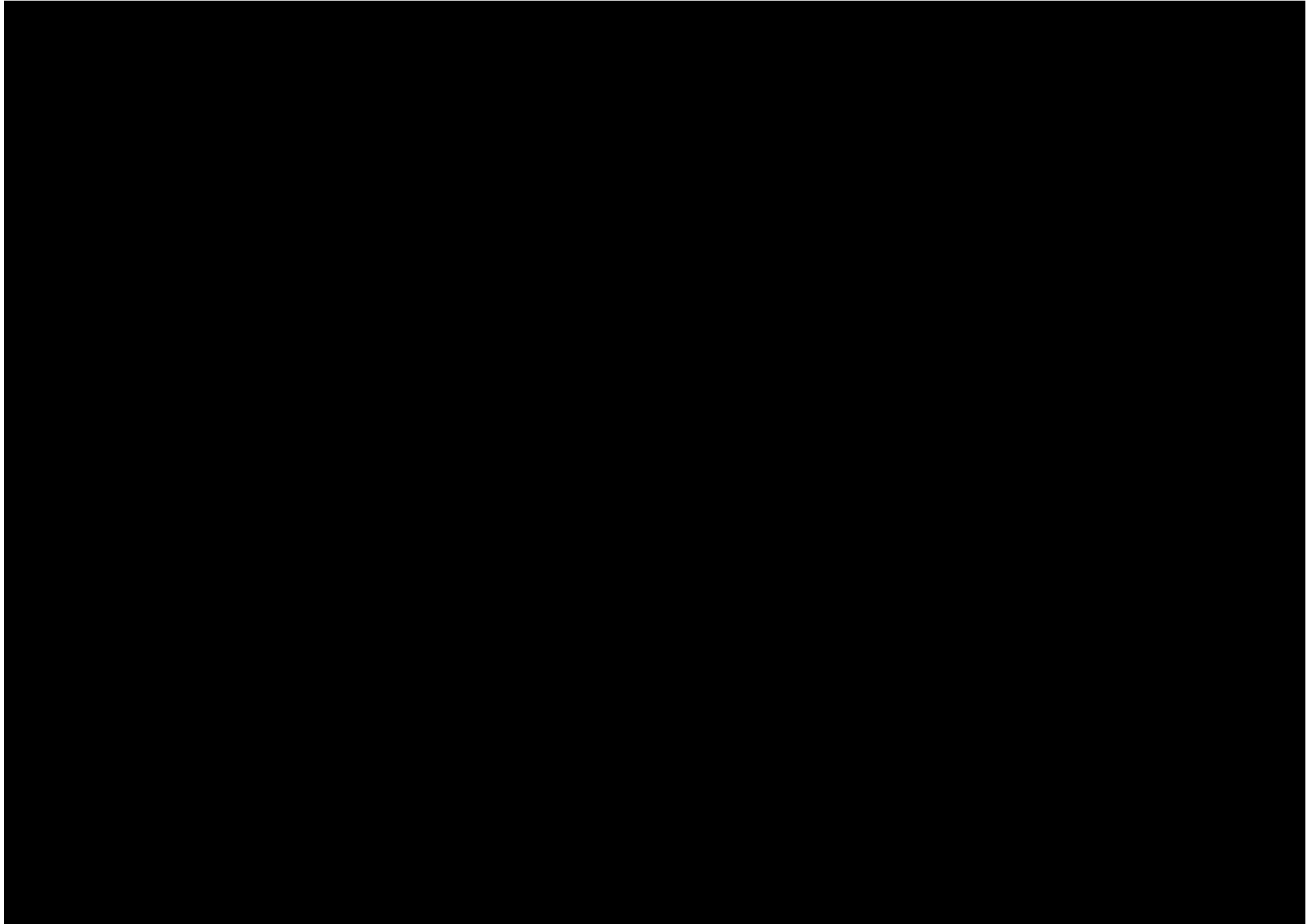
CONFIDENTIAL



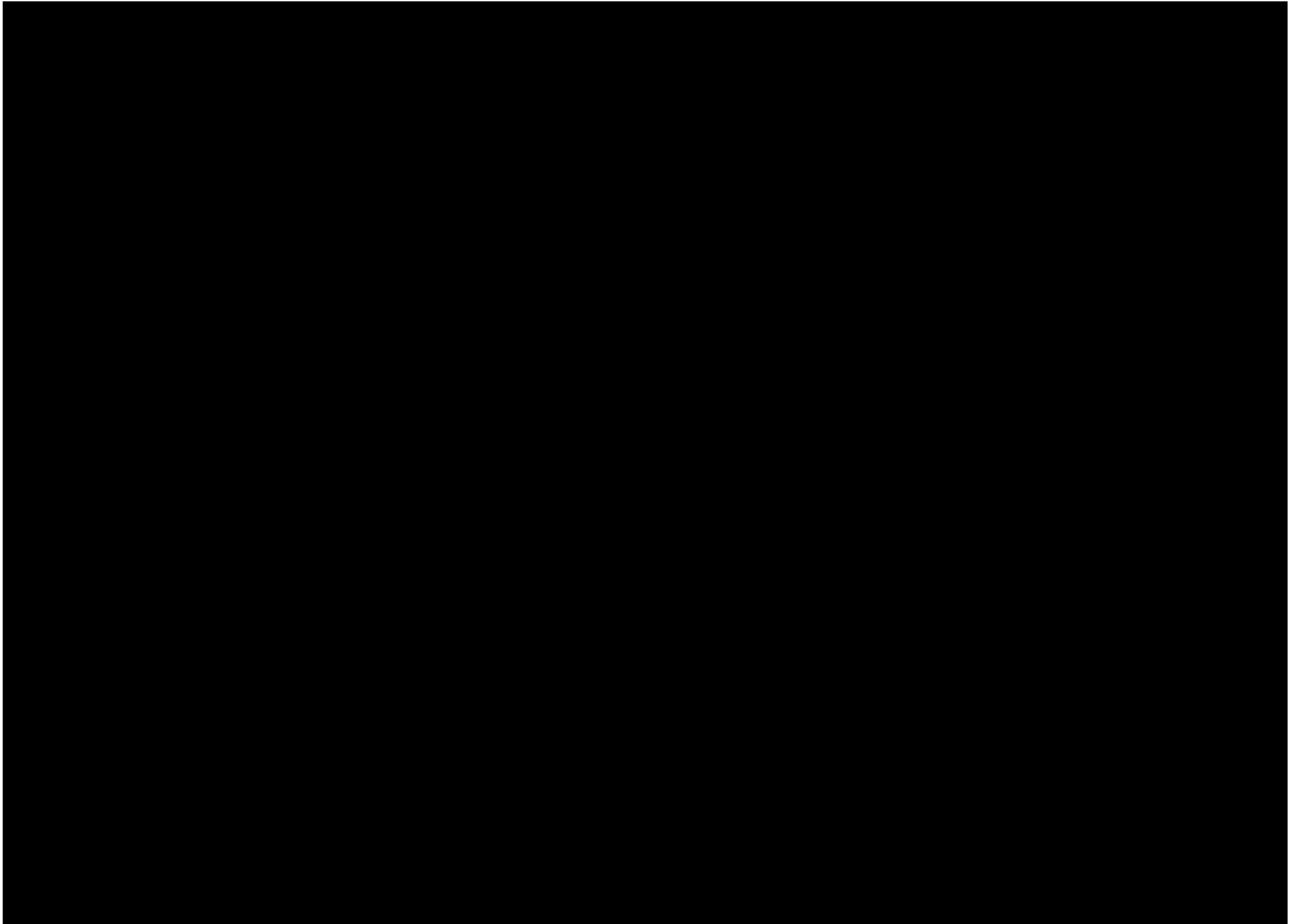
CONFIDENTIAL



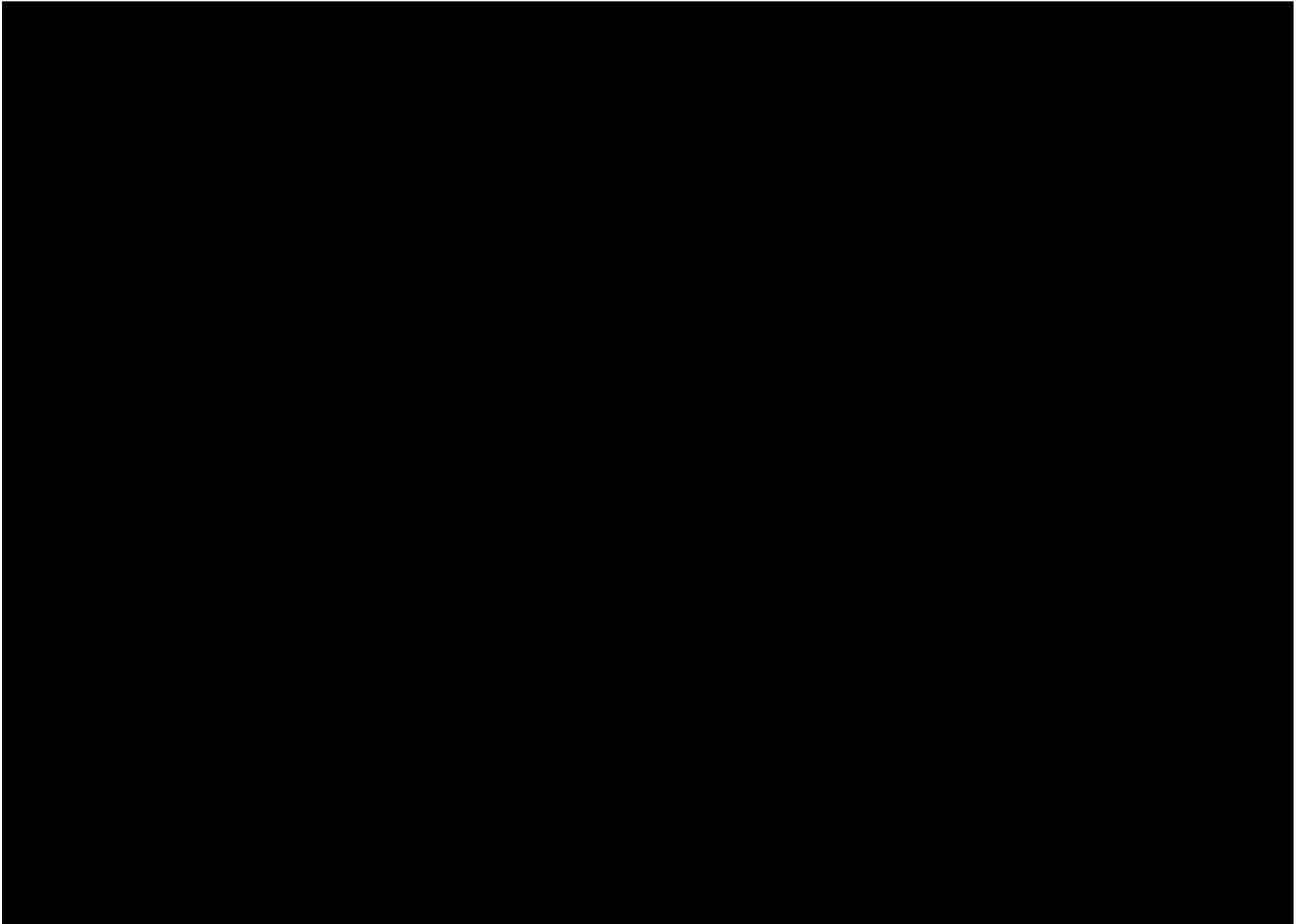
CONFIDENTIAL



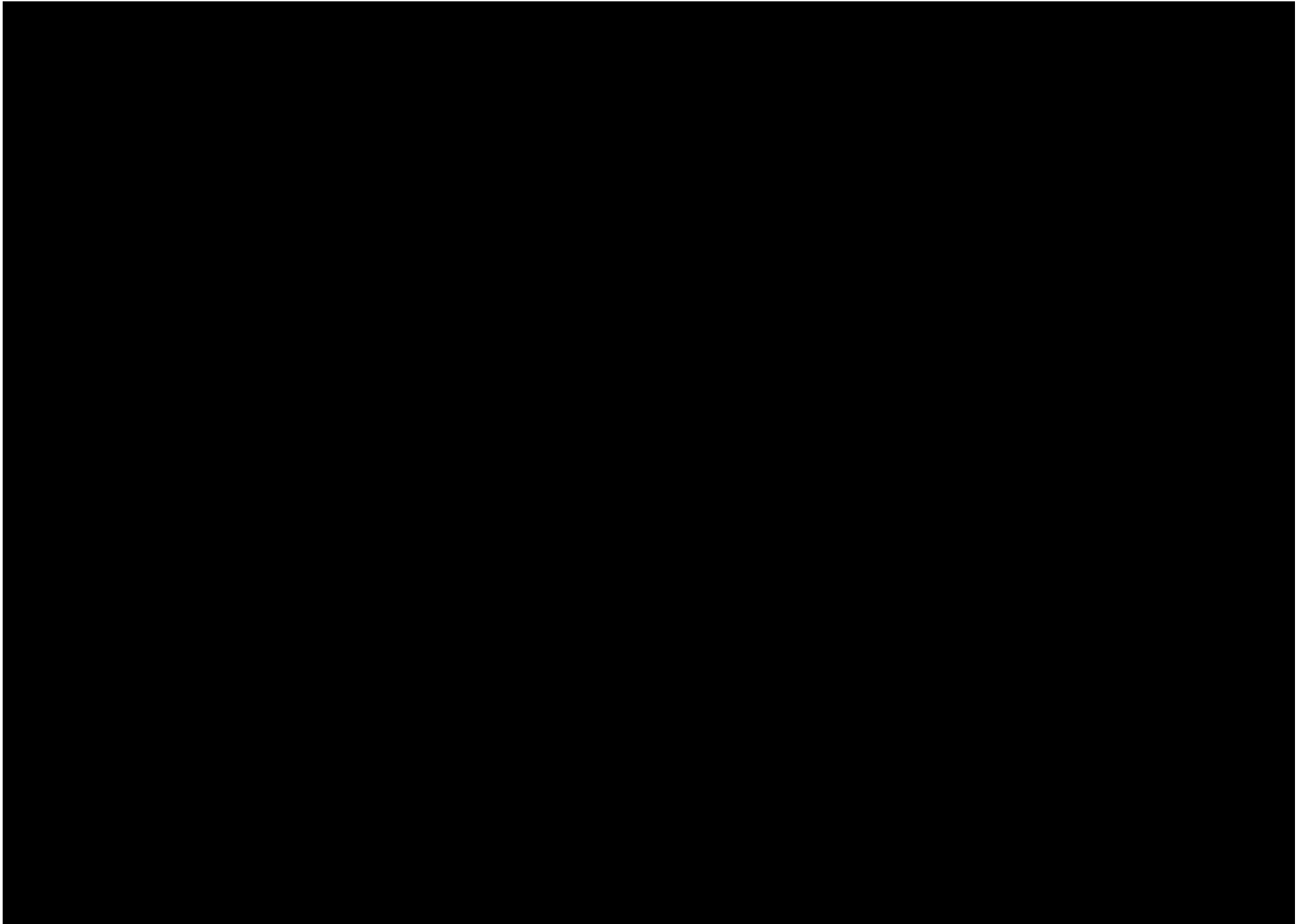
CONFIDENTIAL



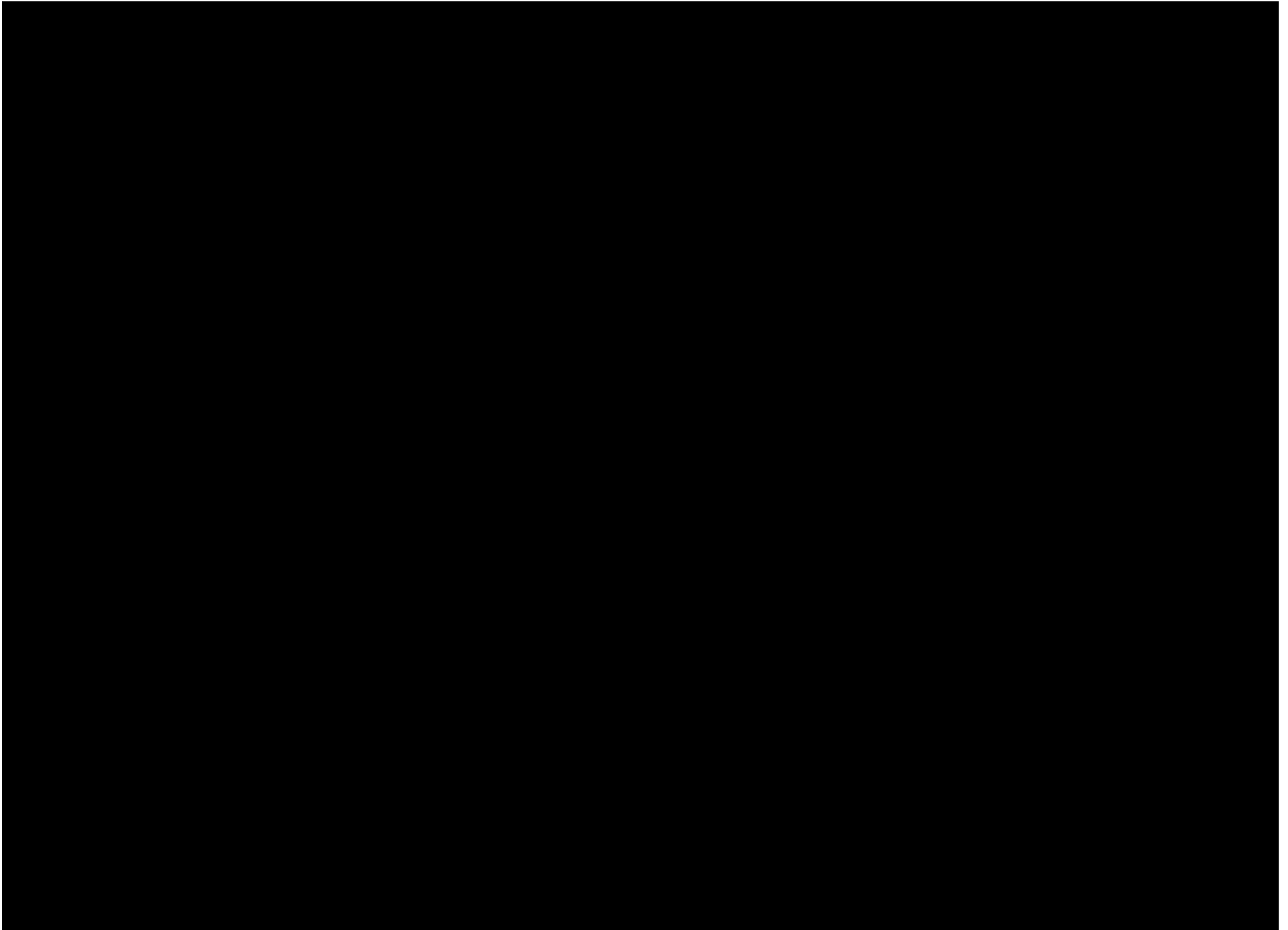
CONFIDENTIAL



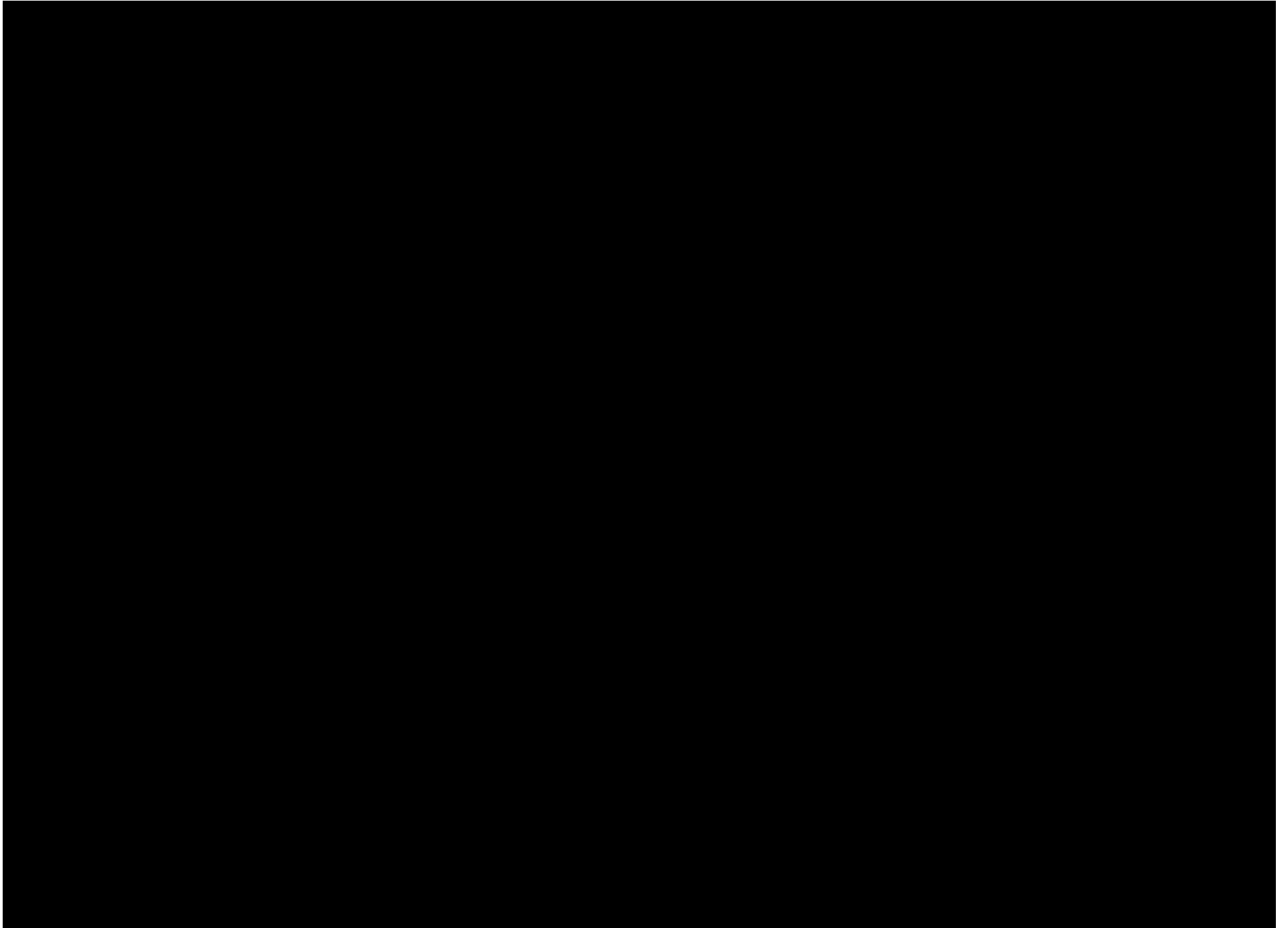
CONFIDENTIAL



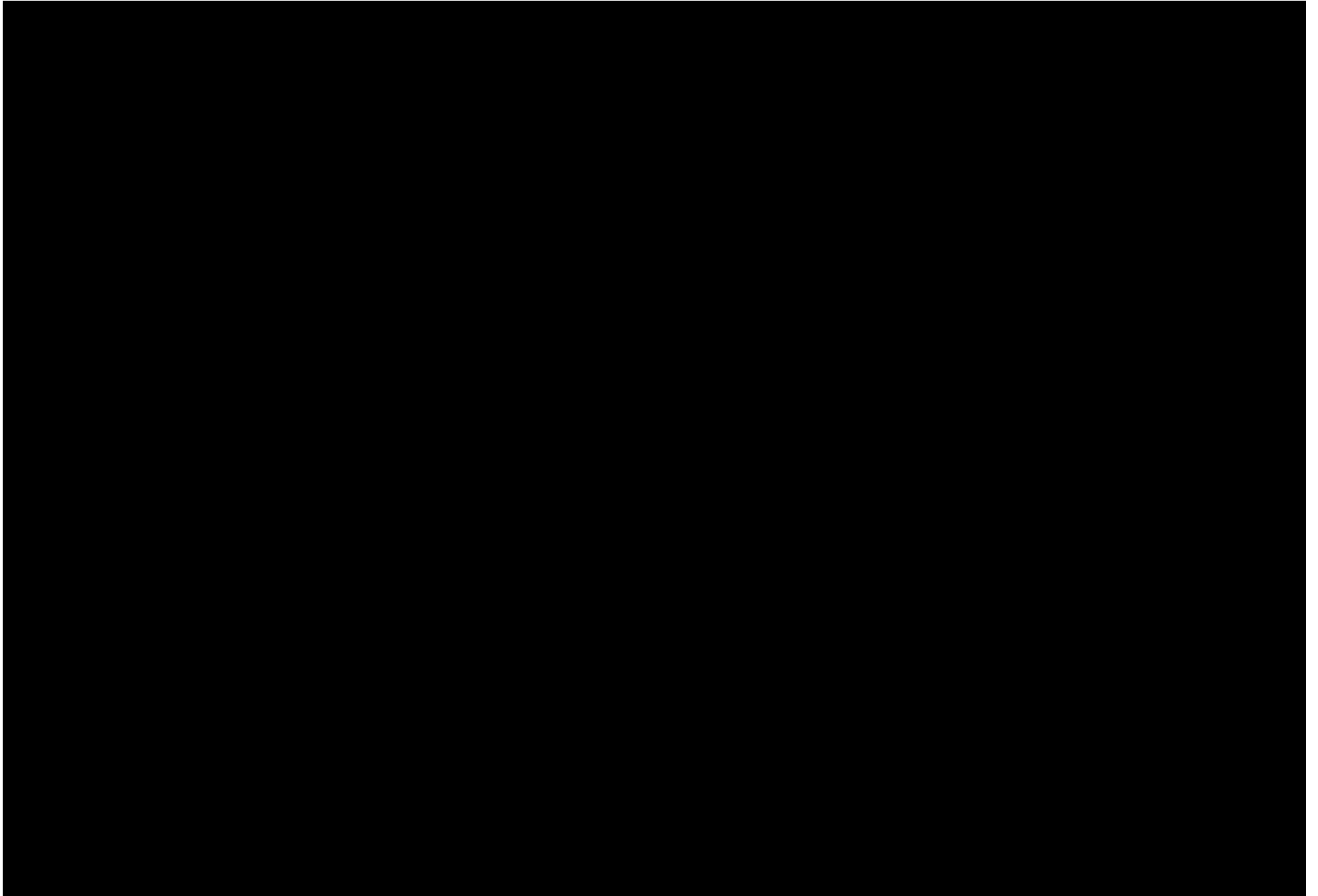
CONFIDENTIAL



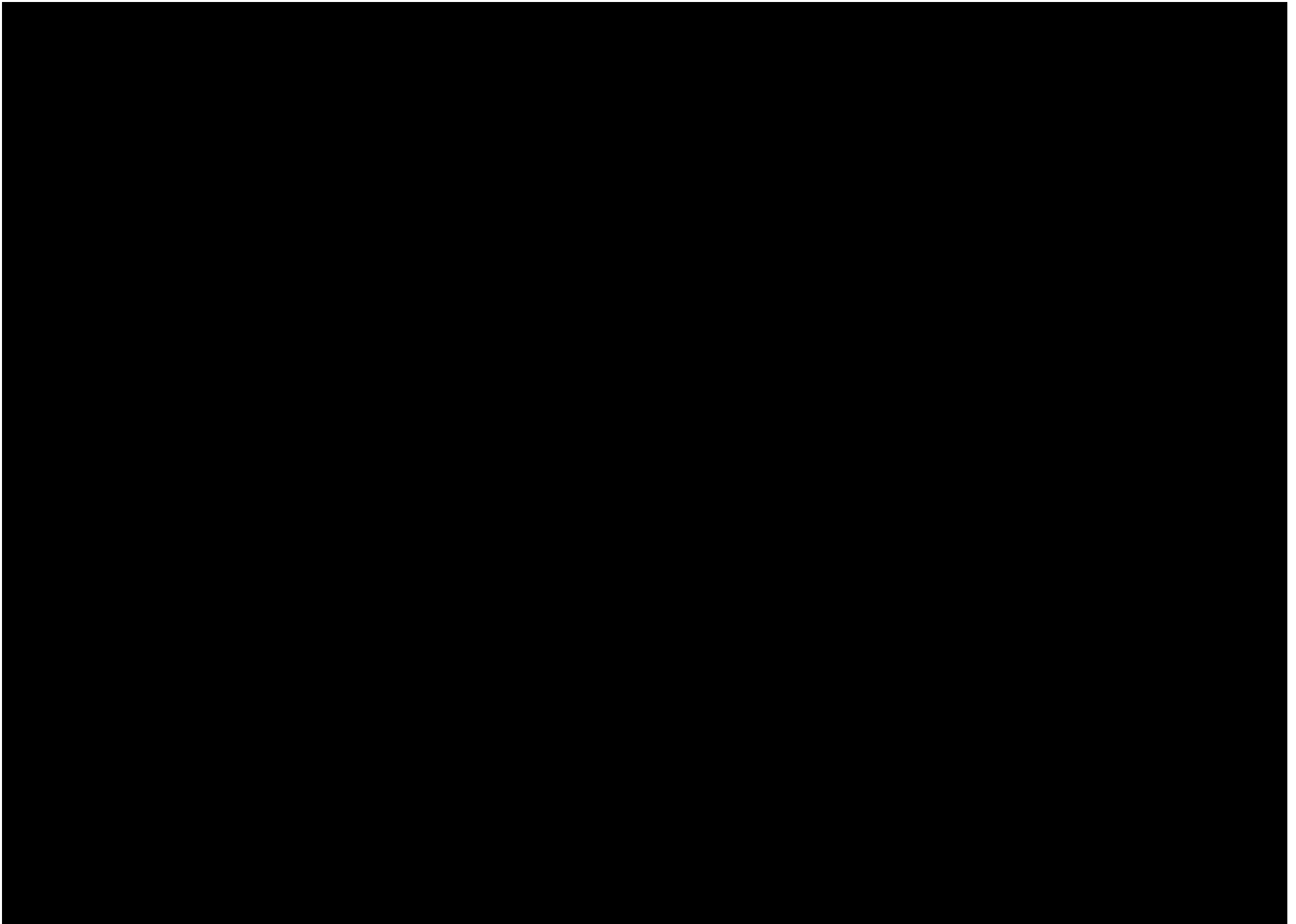
CONFIDENTIAL



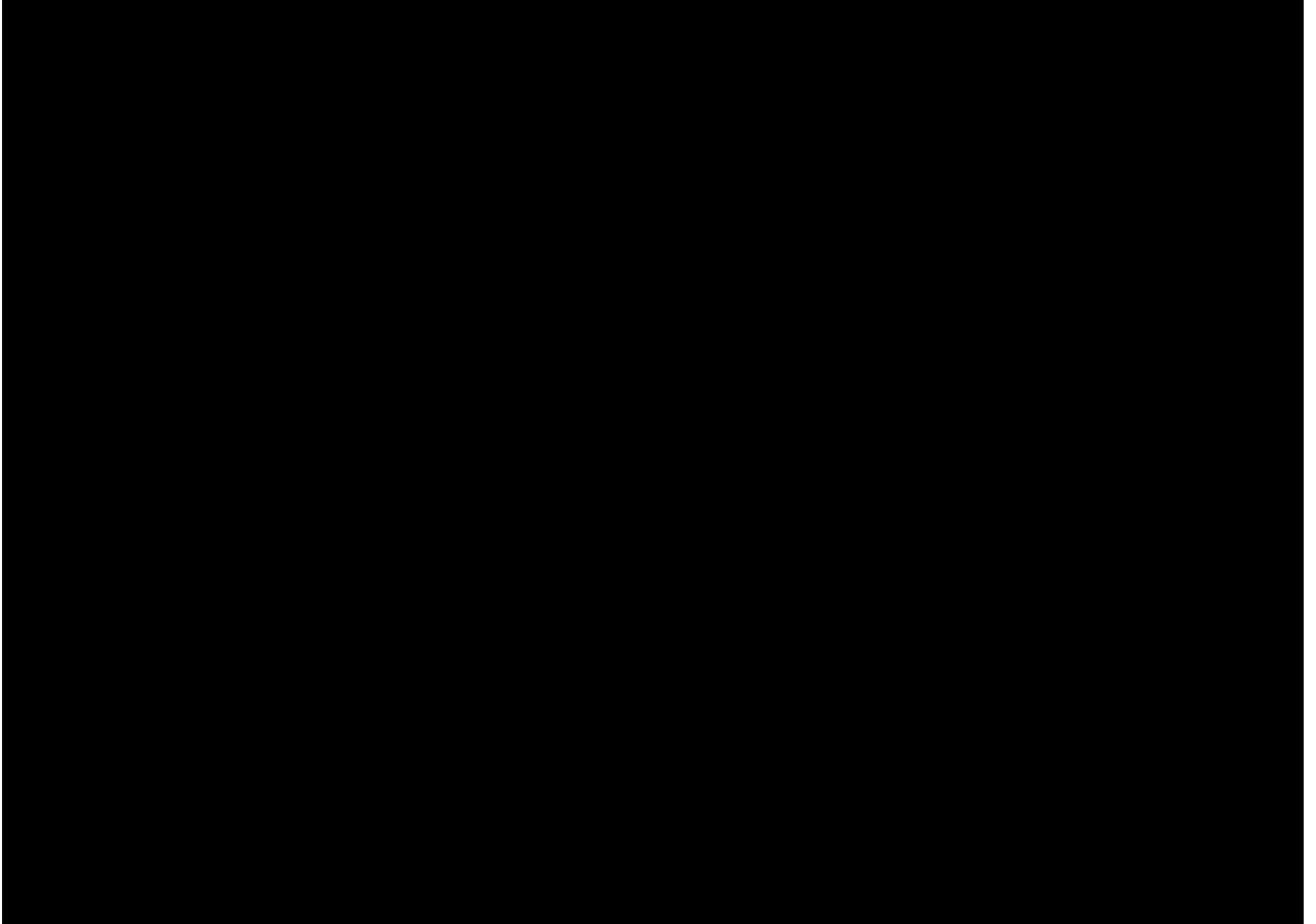
CONFIDENTIAL



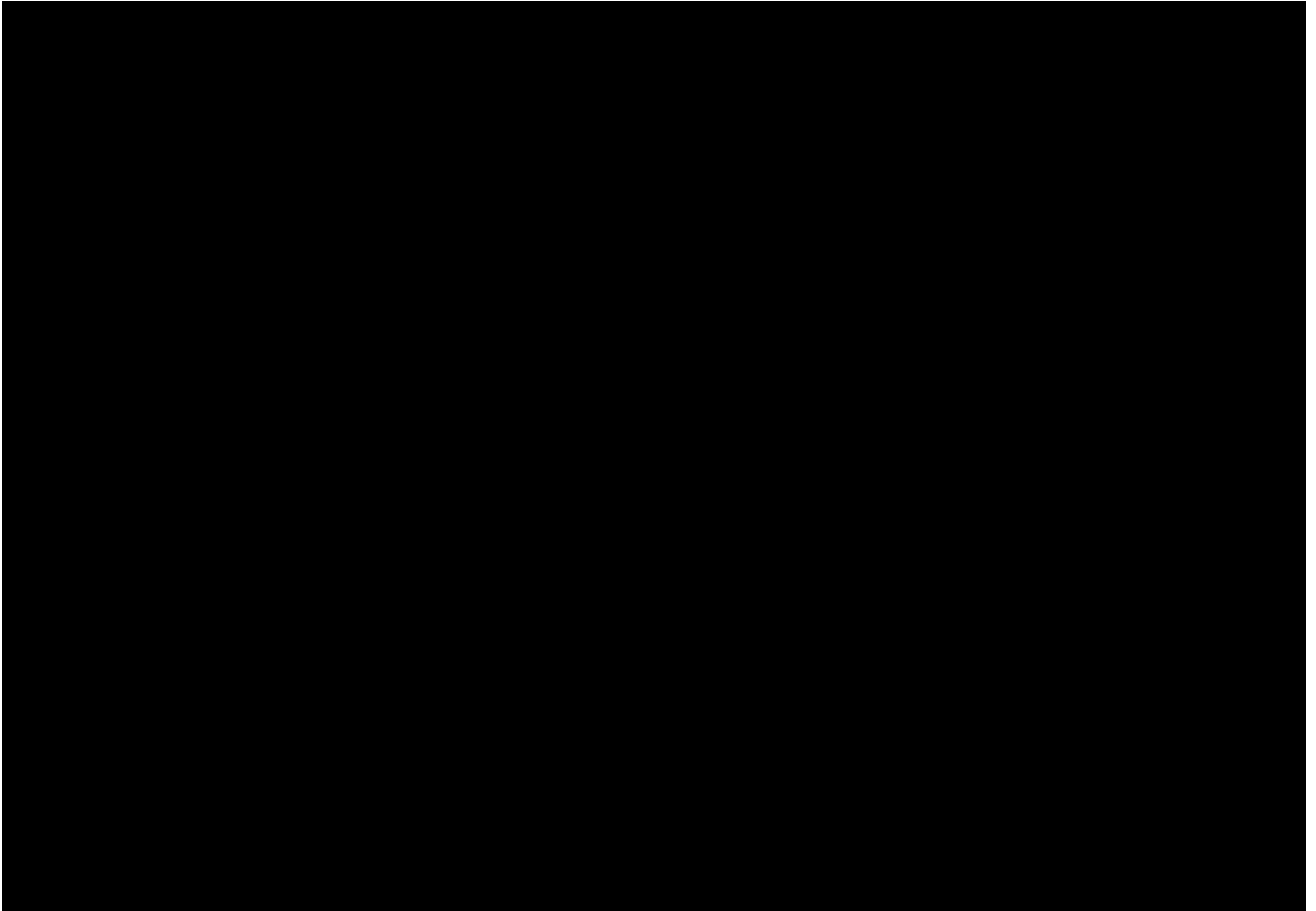
CONFIDENTIAL



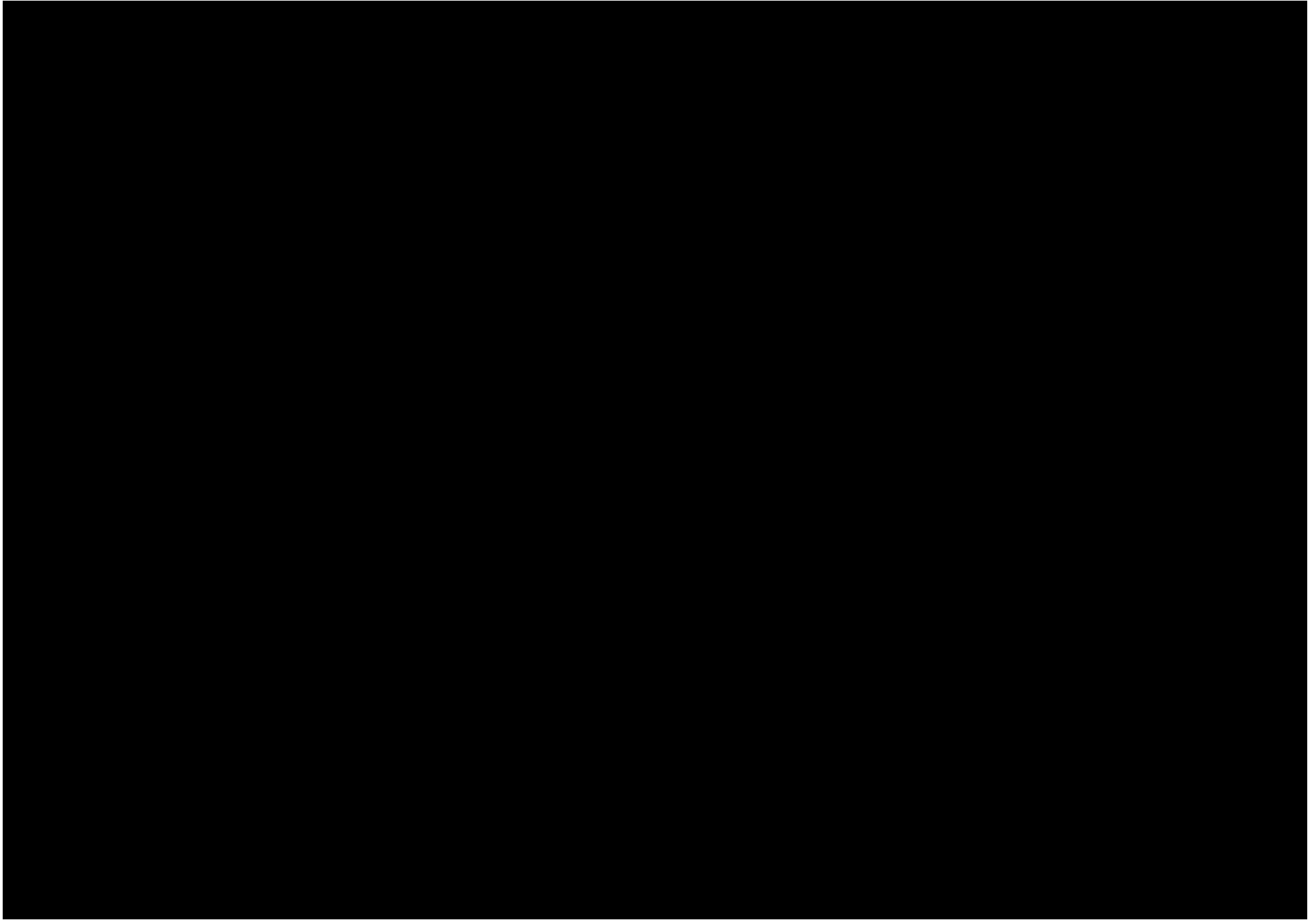
CONFIDENTIAL



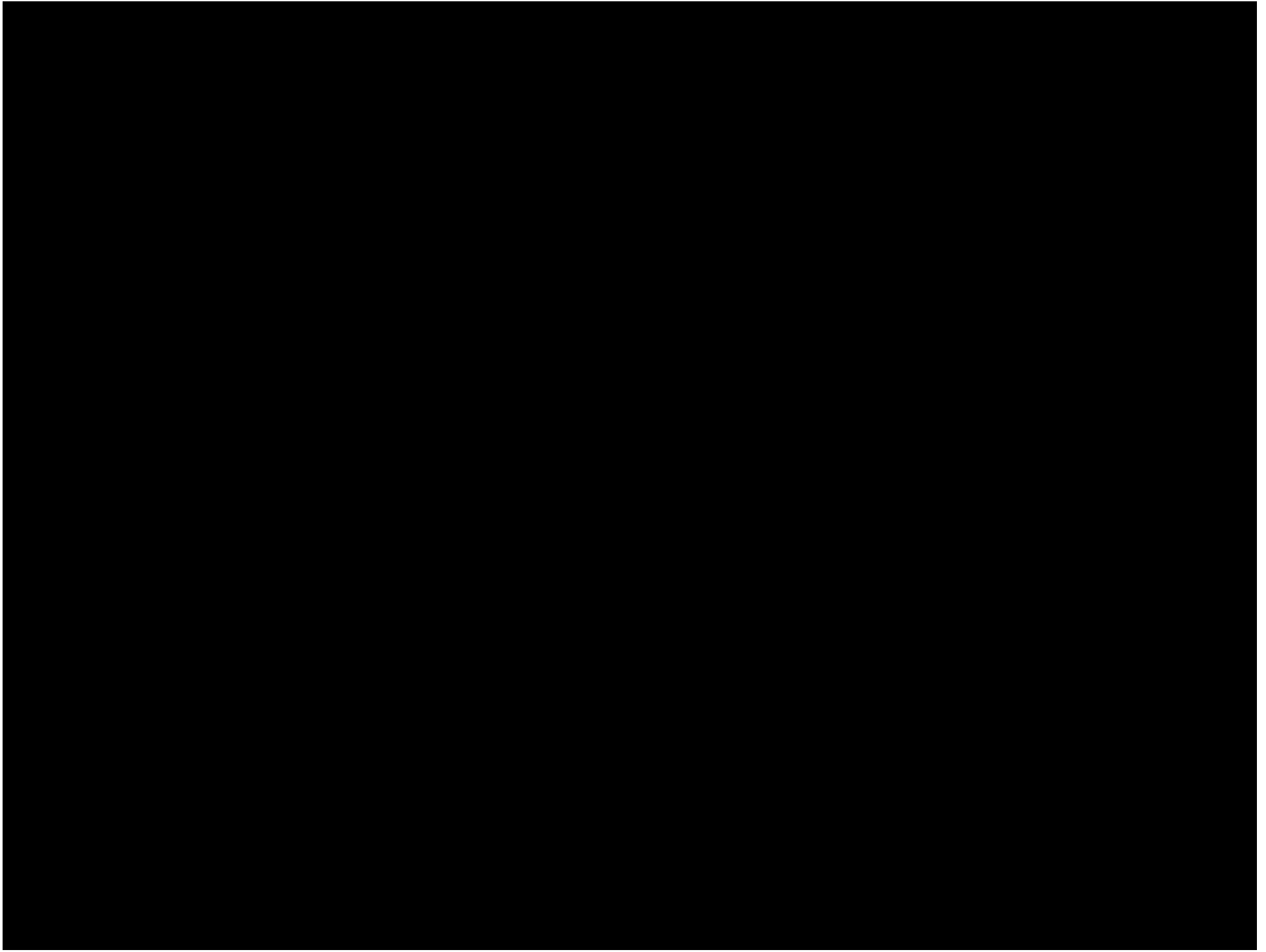
CONFIDENTIAL



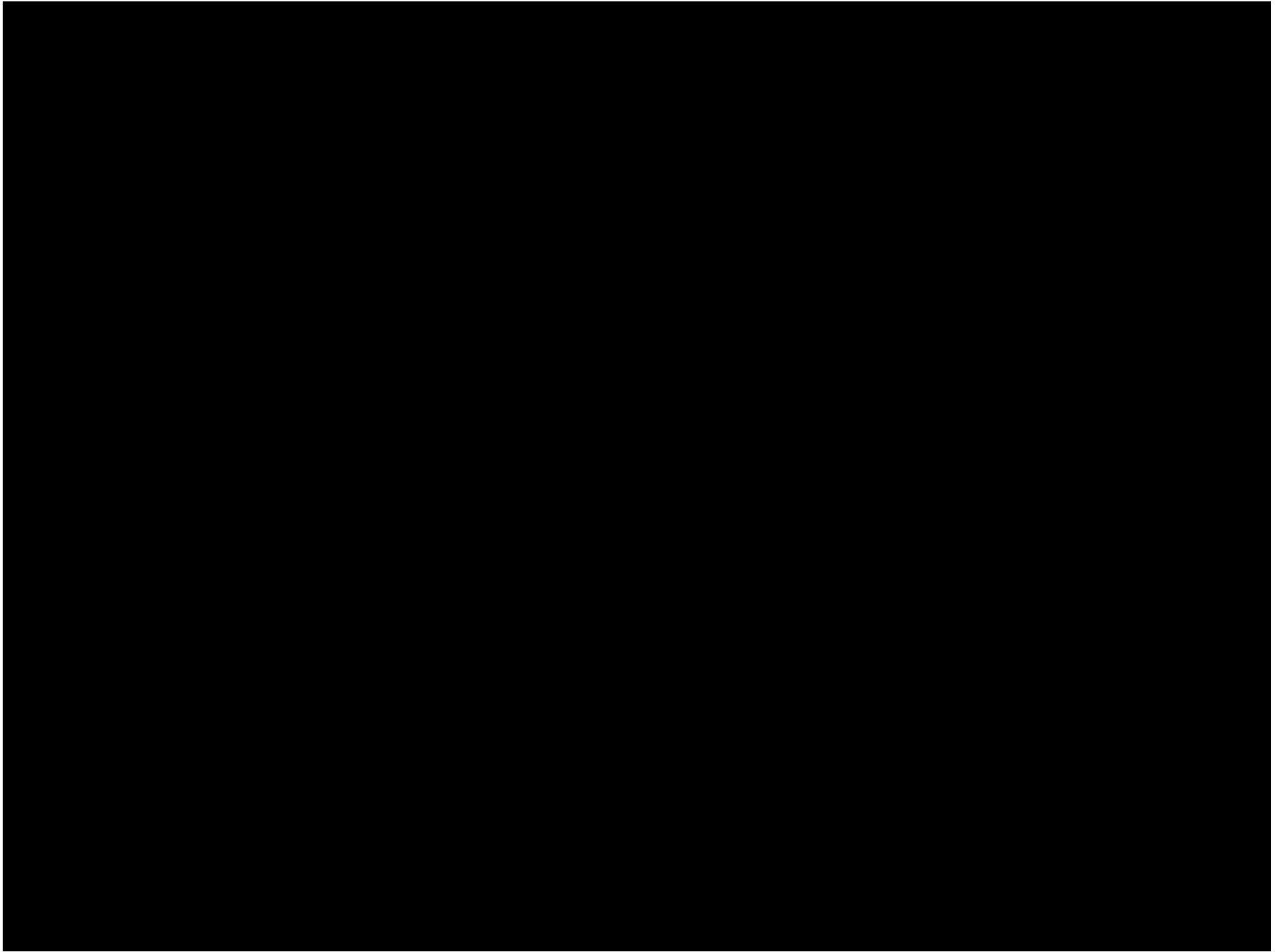
CONFIDENTIAL



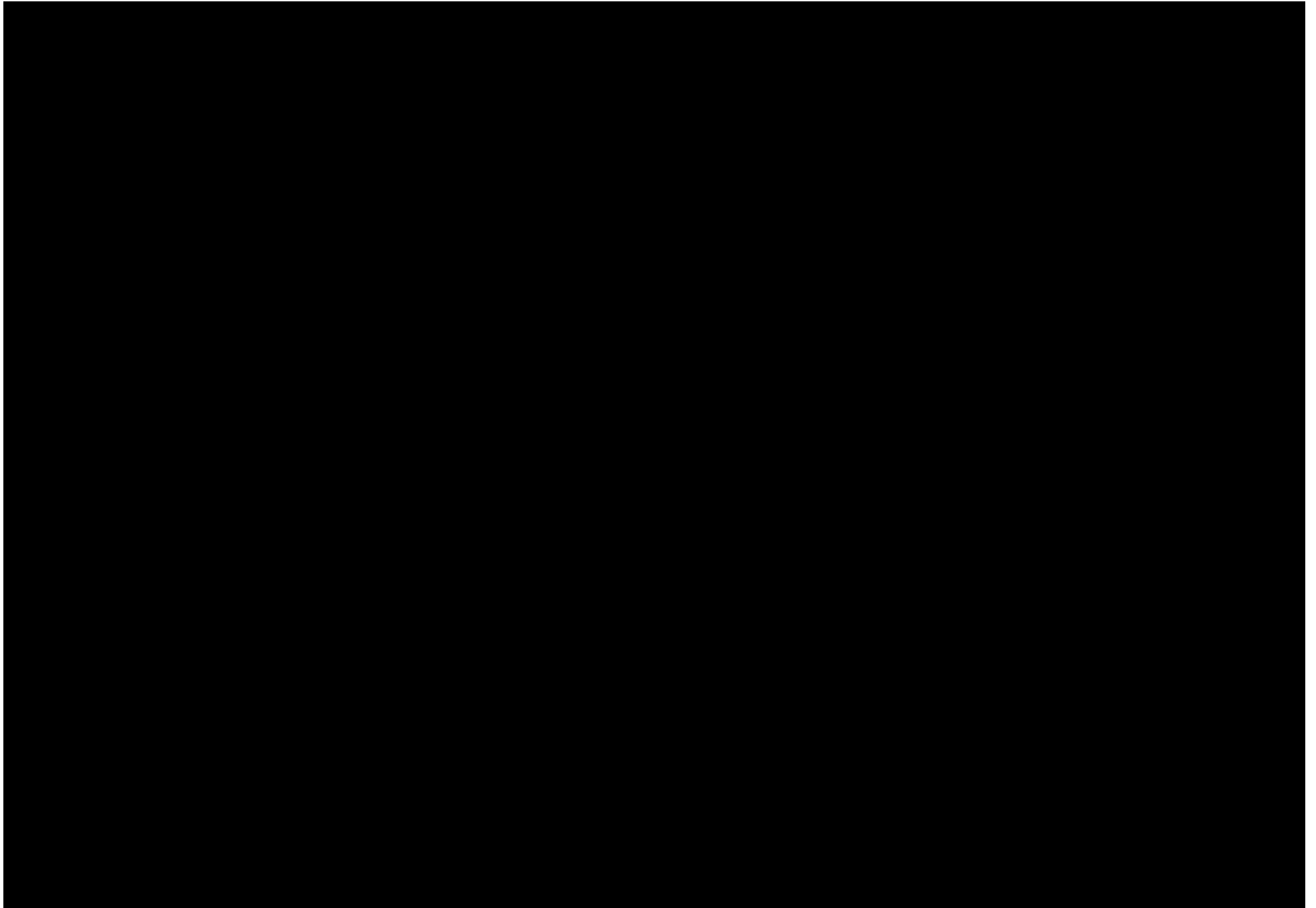
CONFIDENTIAL



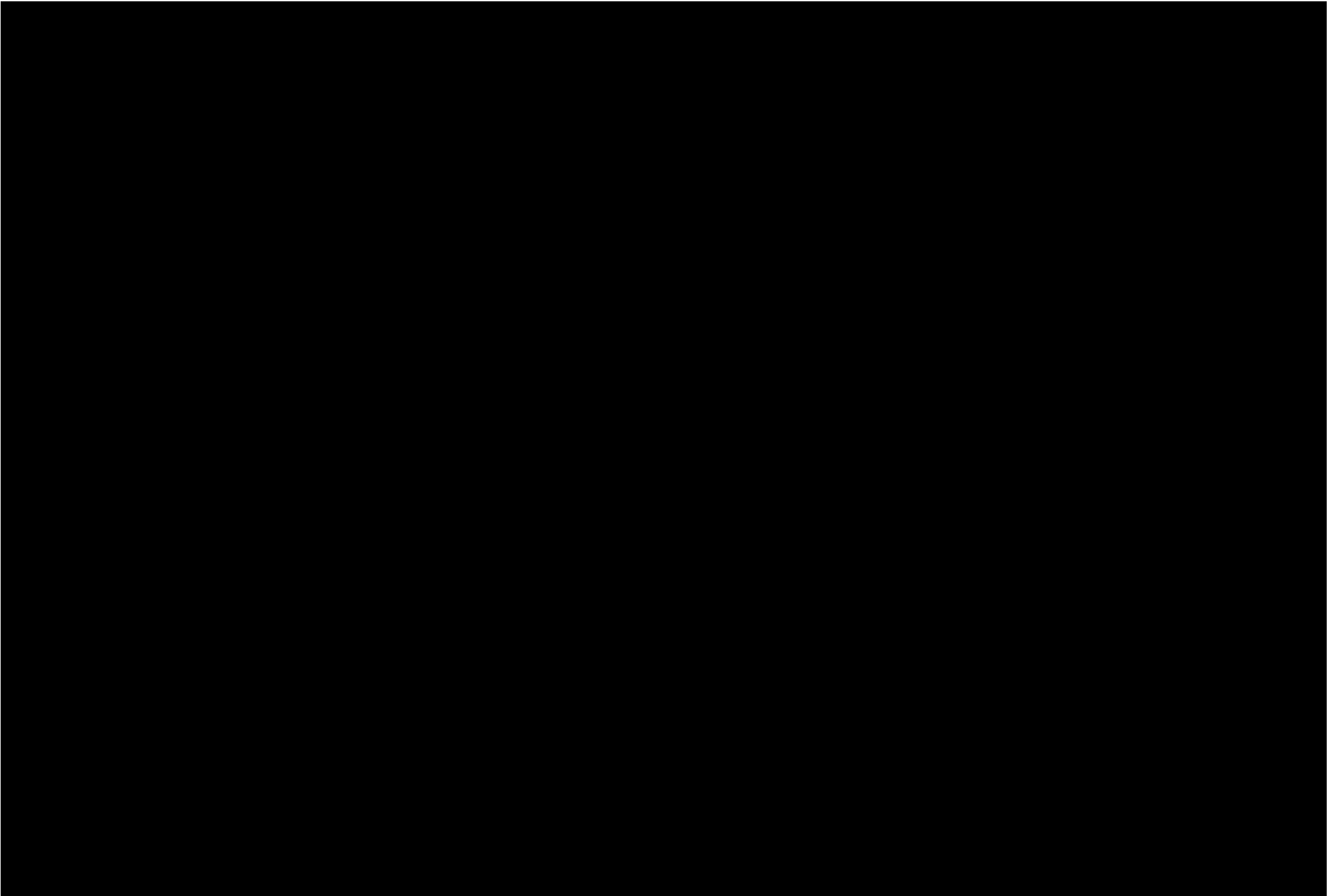
CONFIDENTIAL

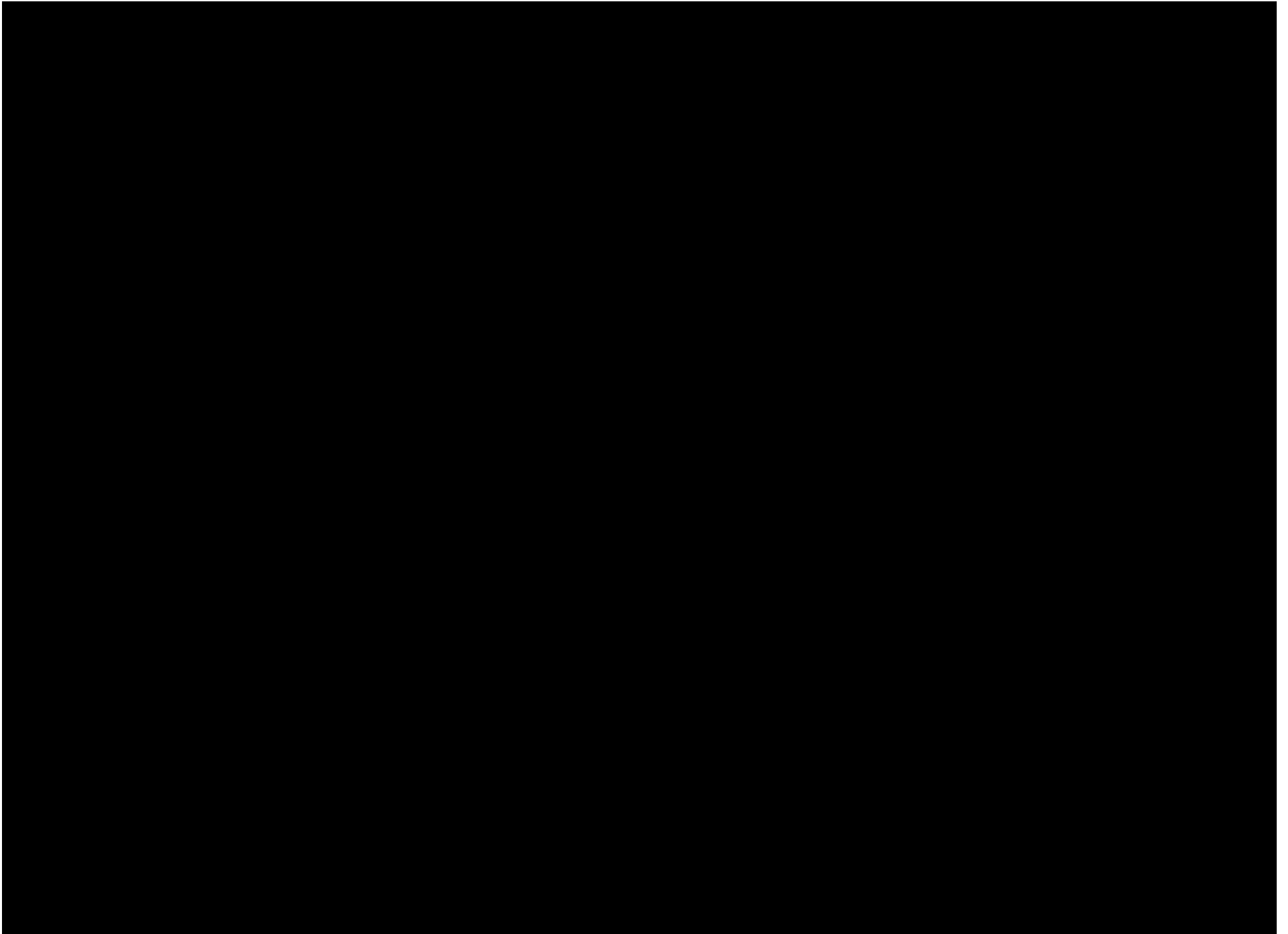


CONFIDENTIAL

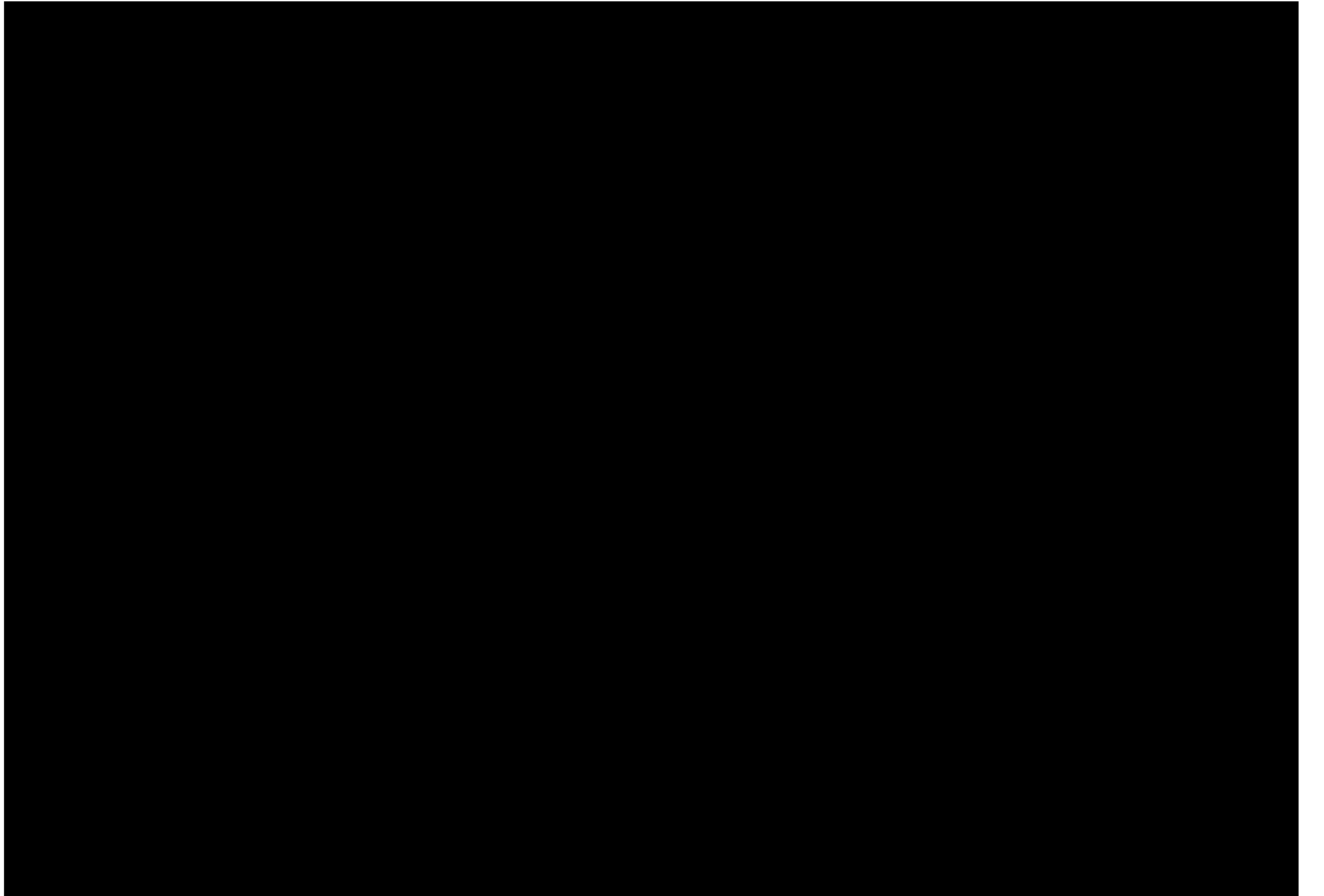


CONFIDENTIAL

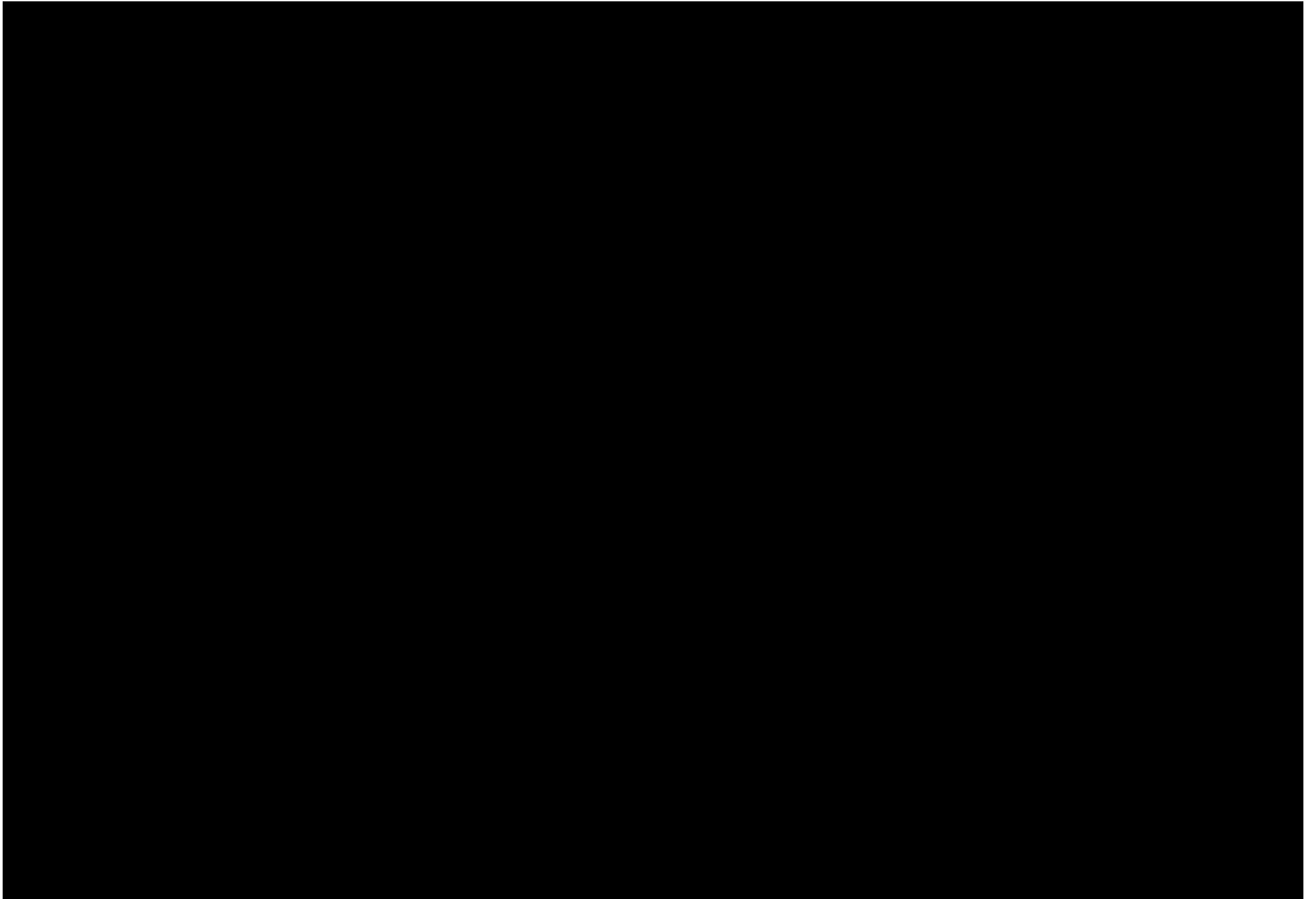




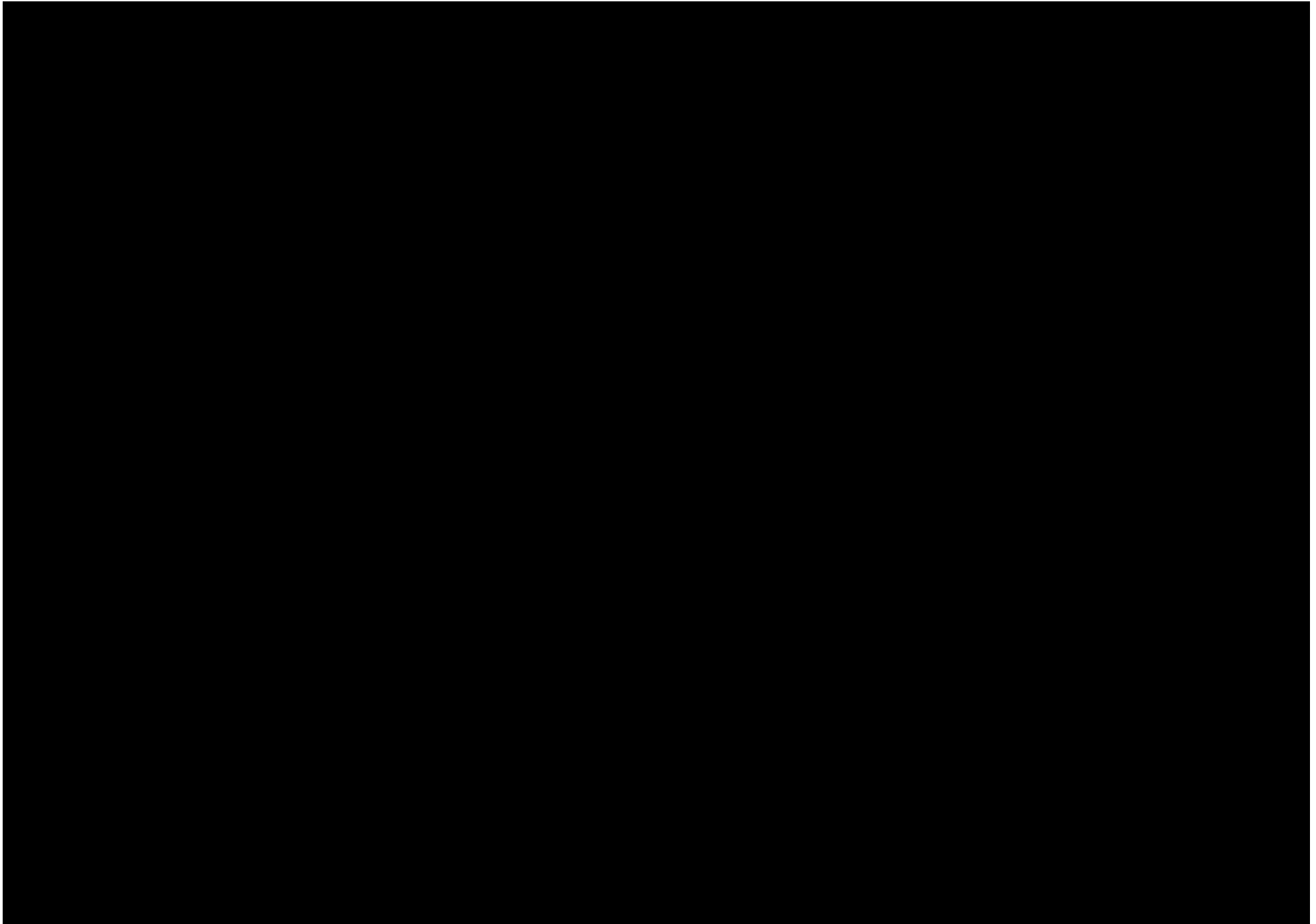
CONFIDENTIAL



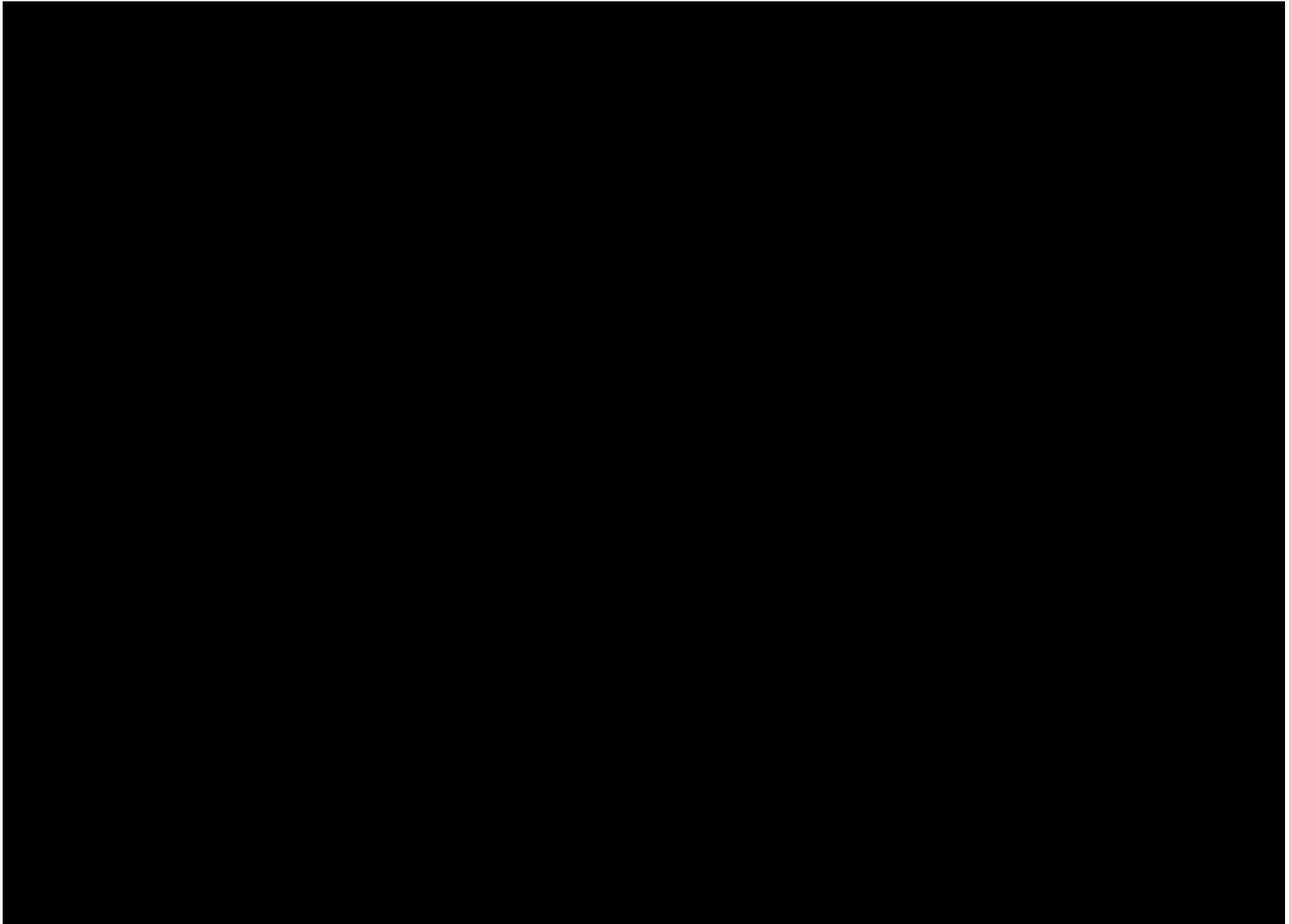
CONFIDENTIAL



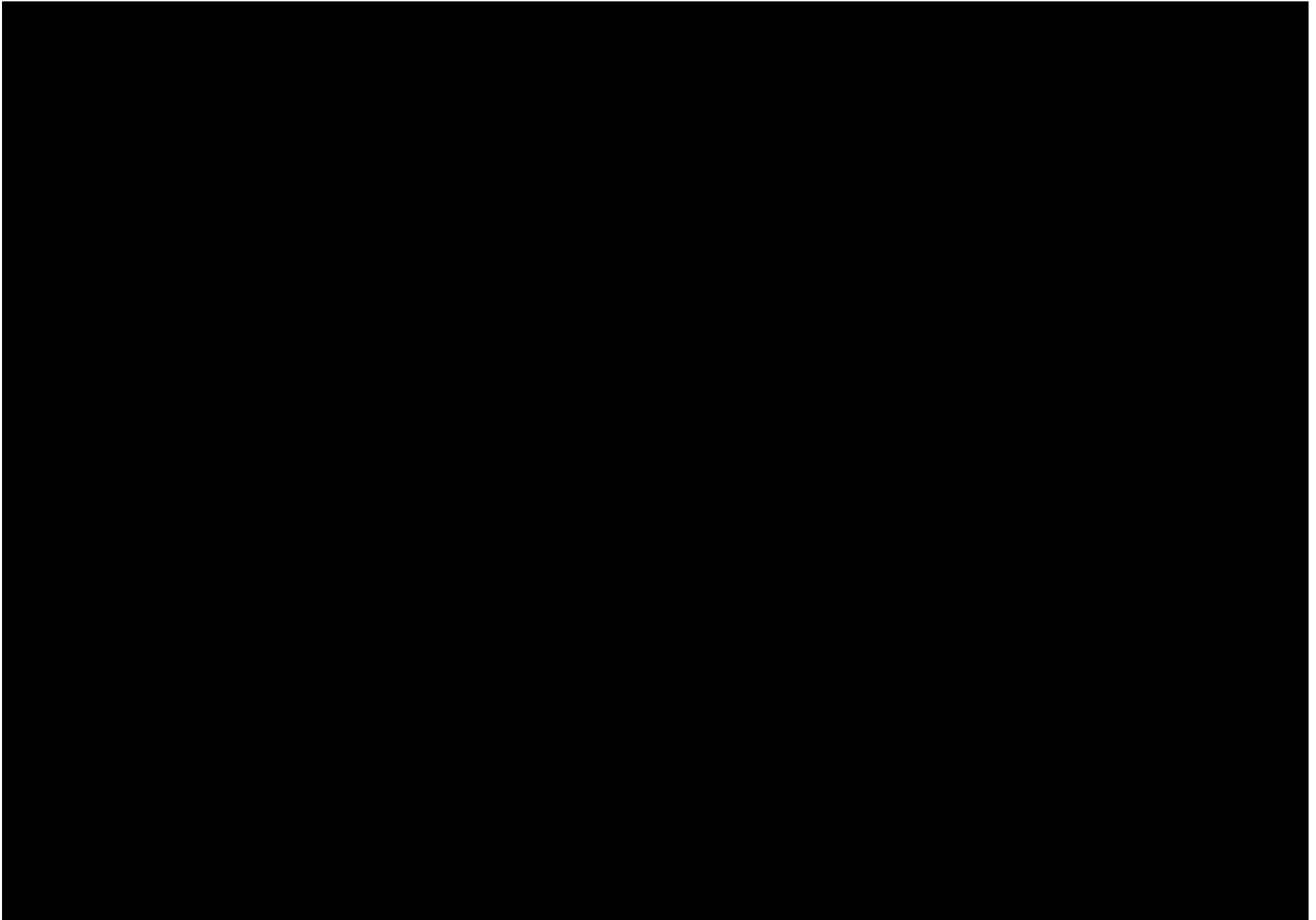
CONFIDENTIAL



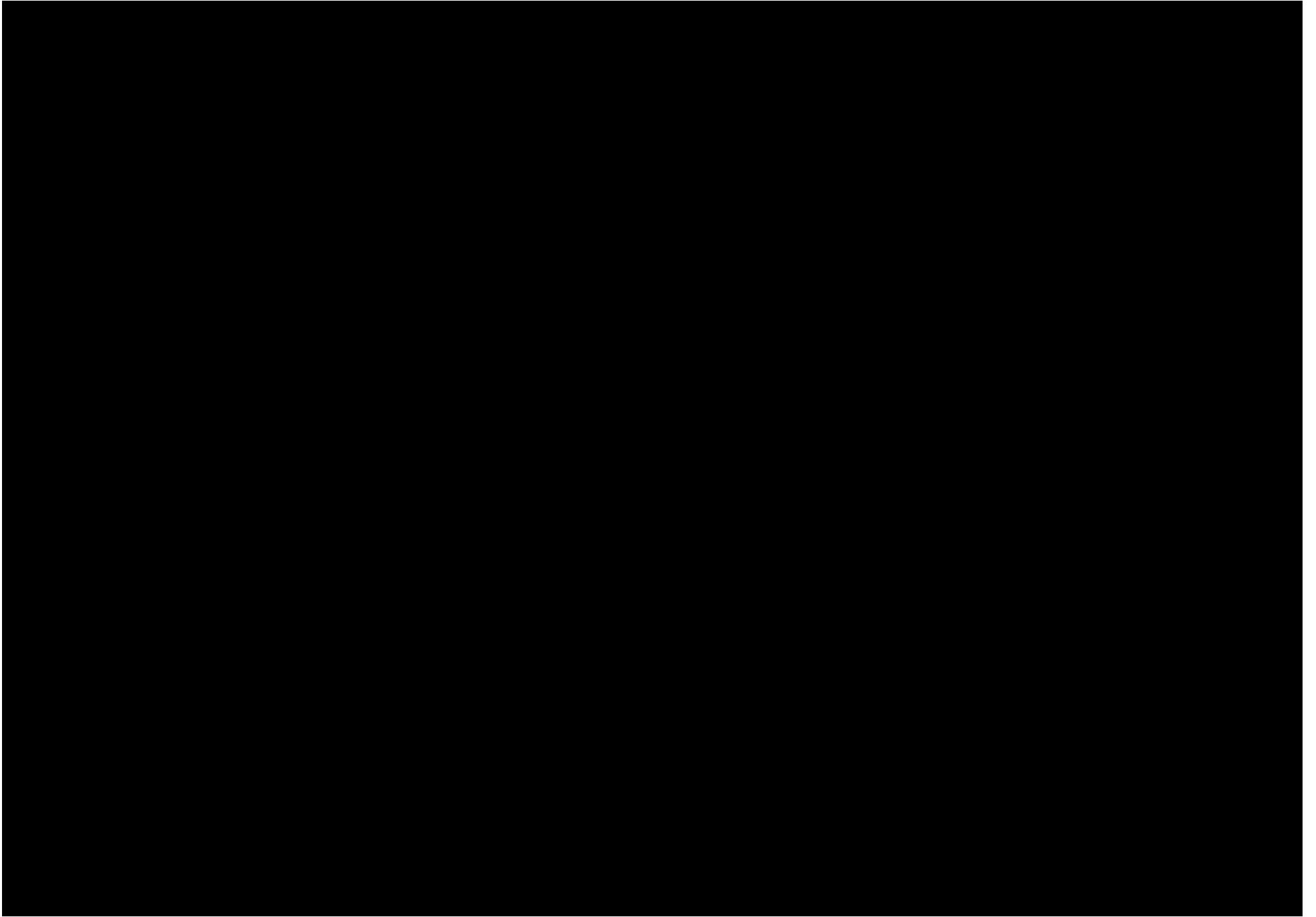
CONFIDENTIAL



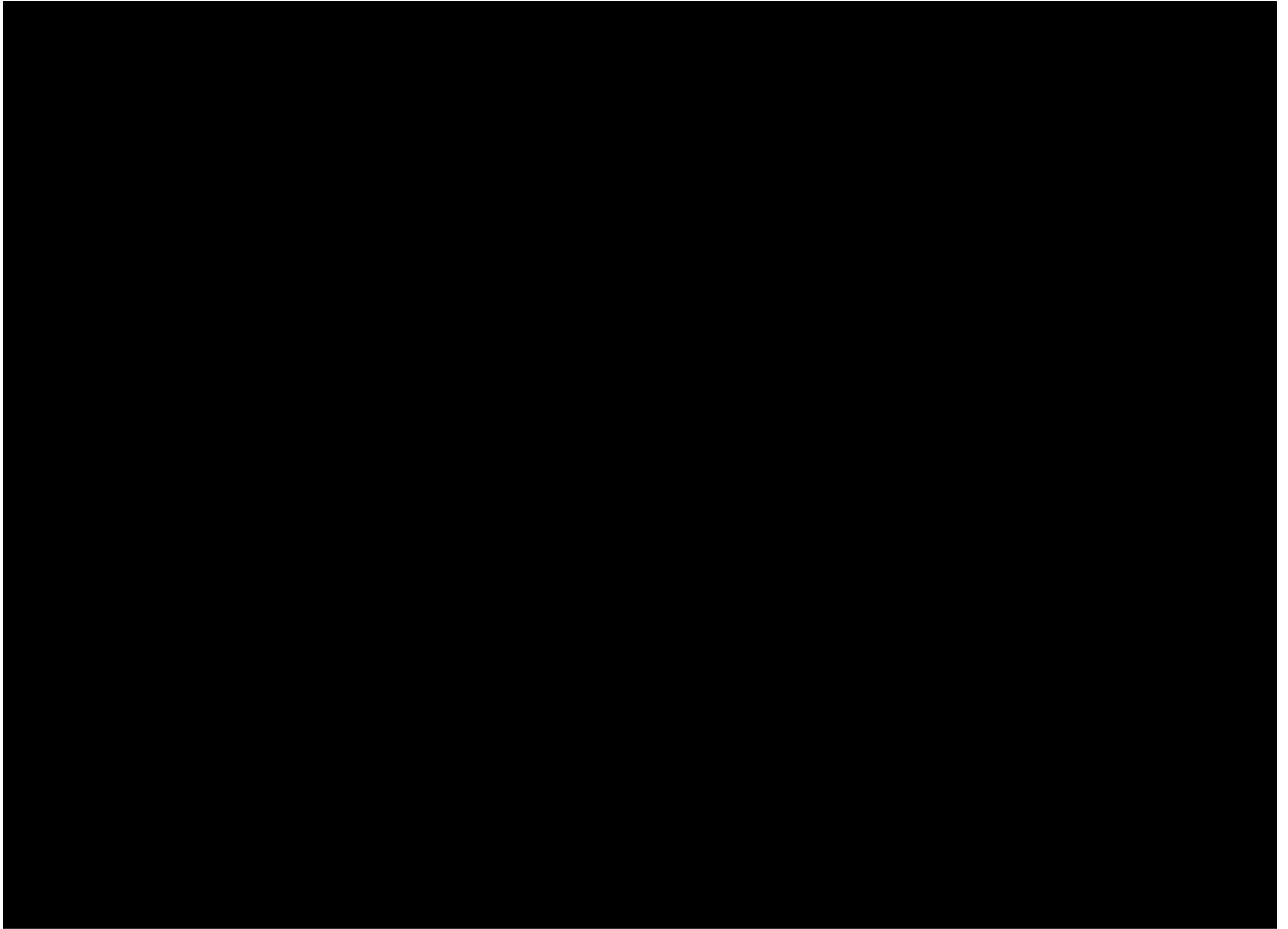
CONFIDENTIAL



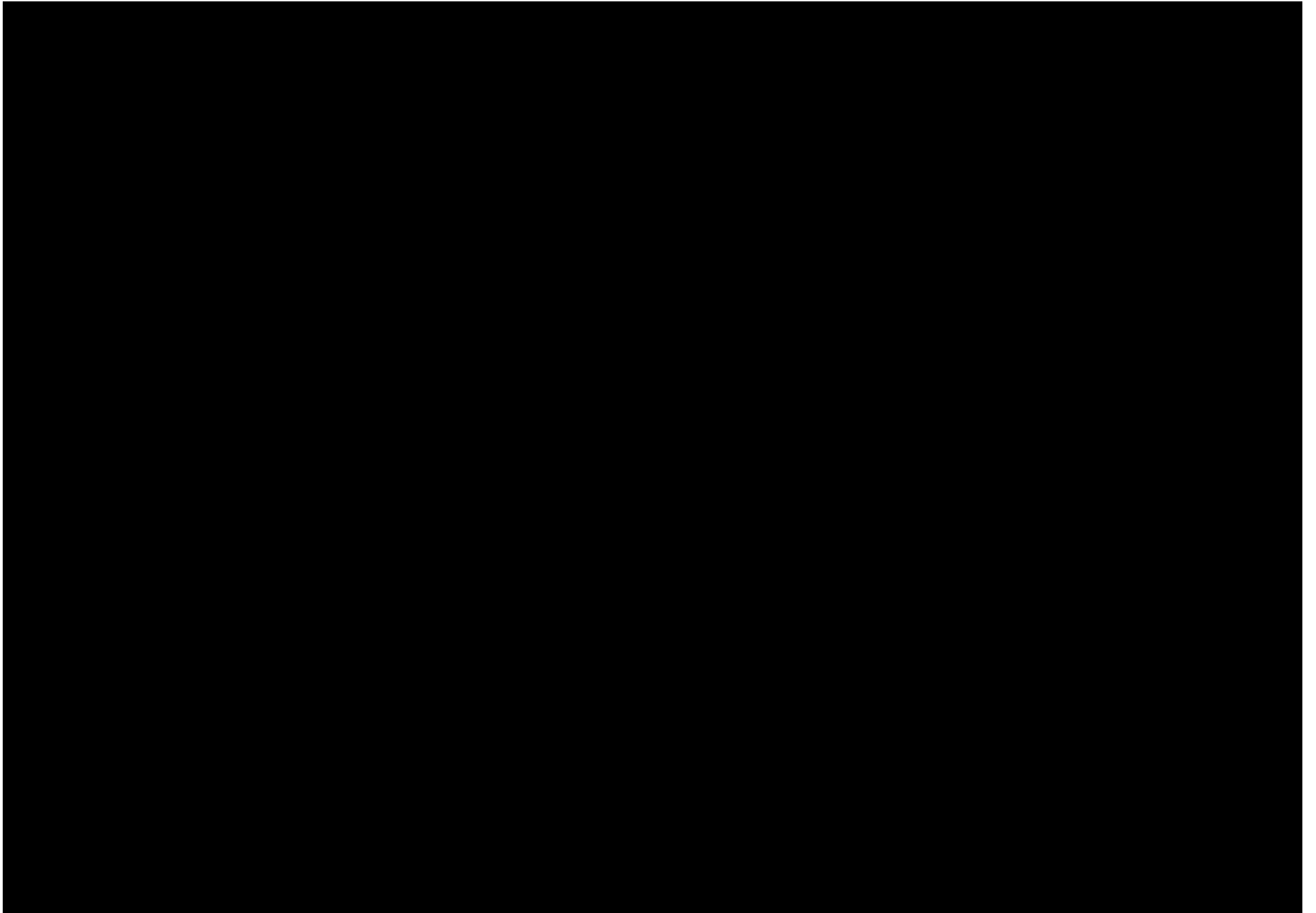
CONFIDENTIAL

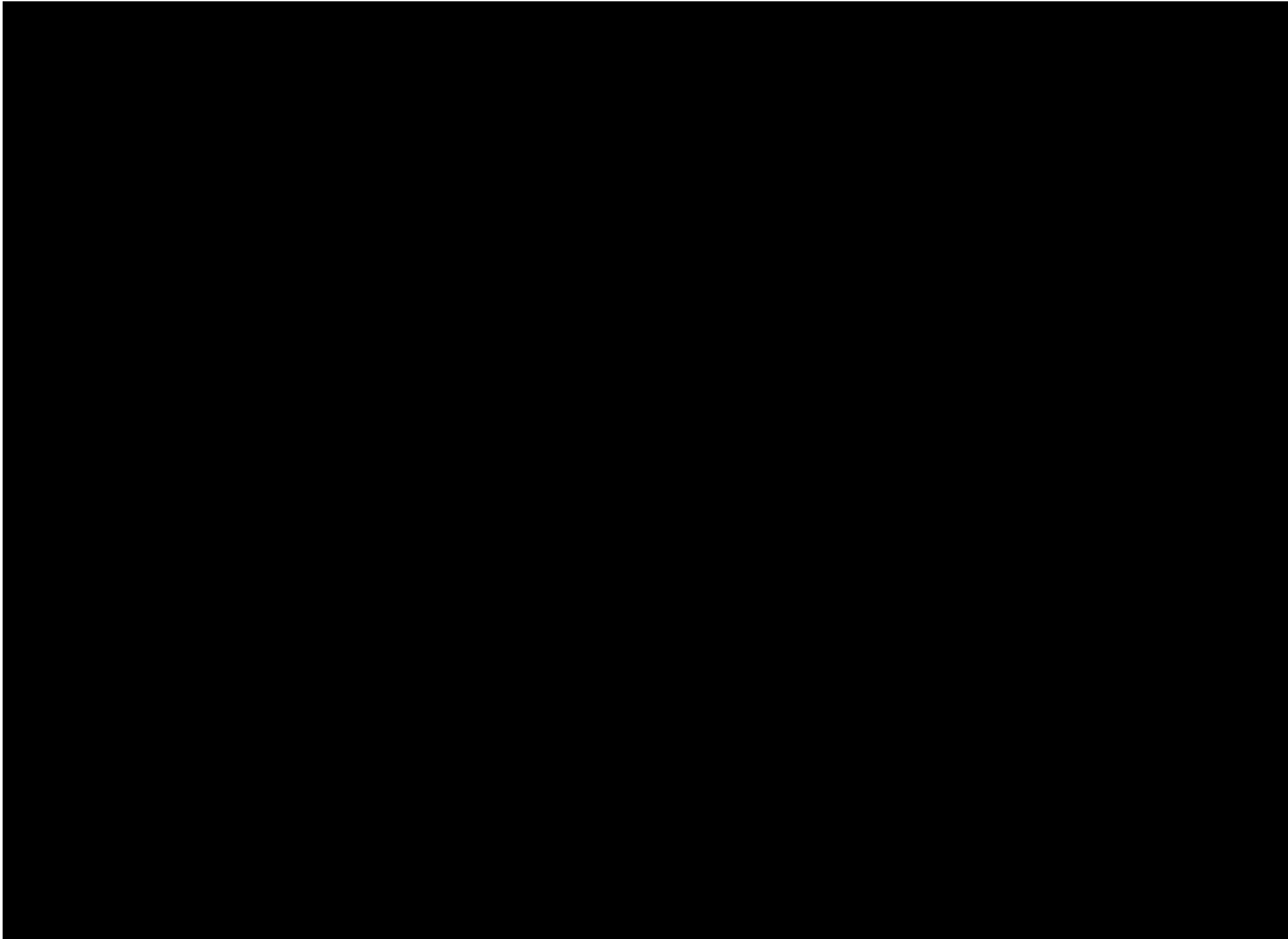


CONFIDENTIAL

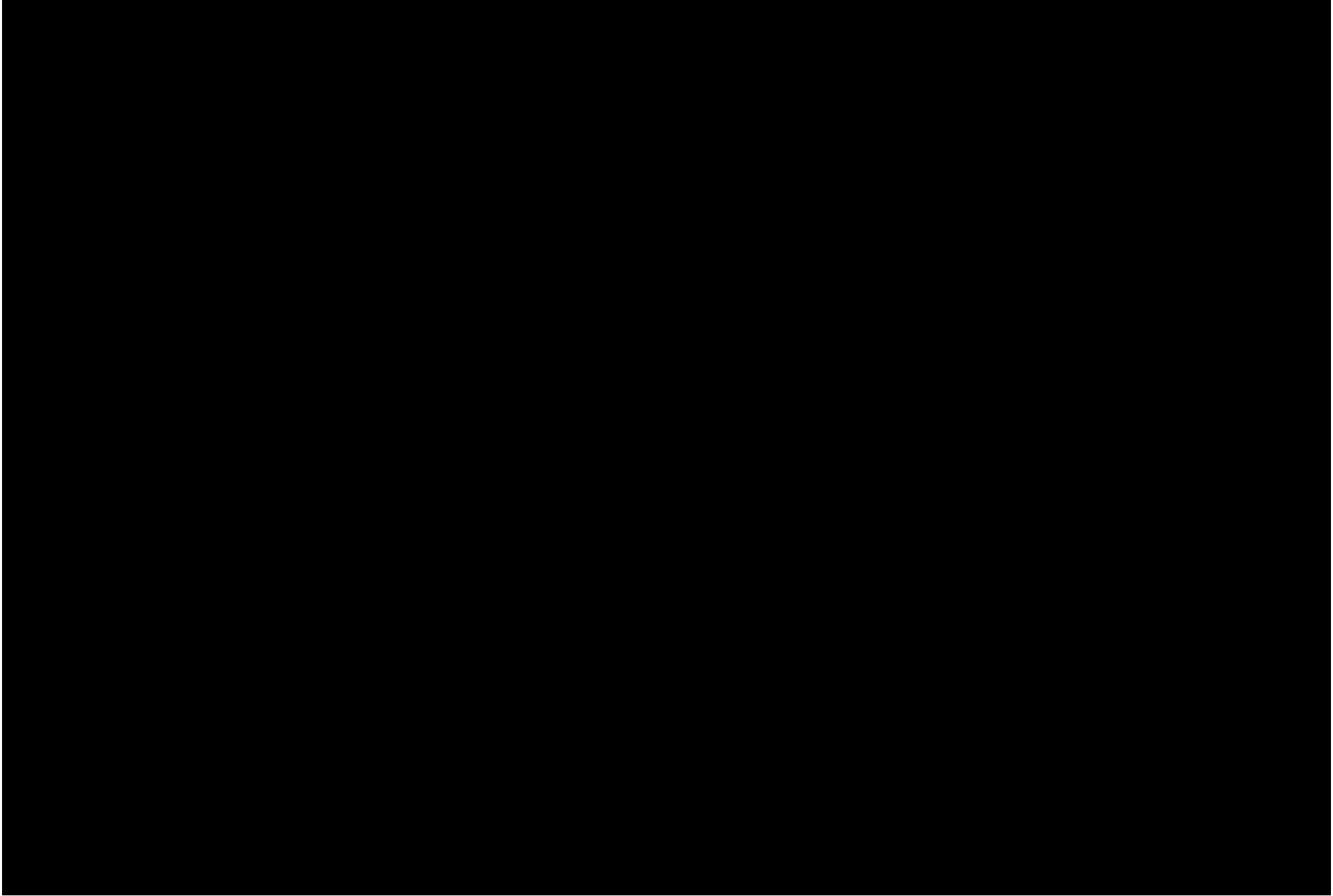


CONFIDENTIAL

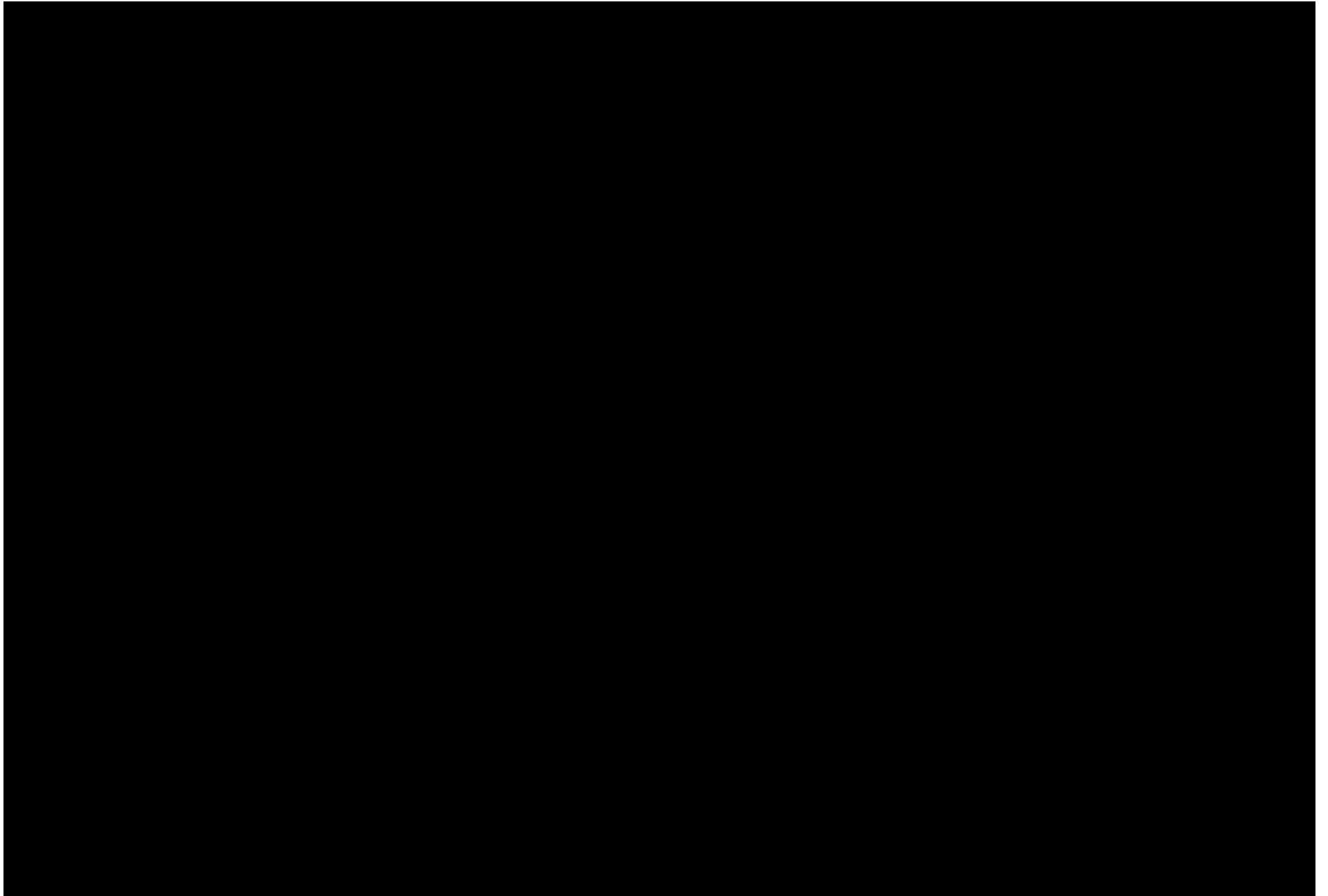


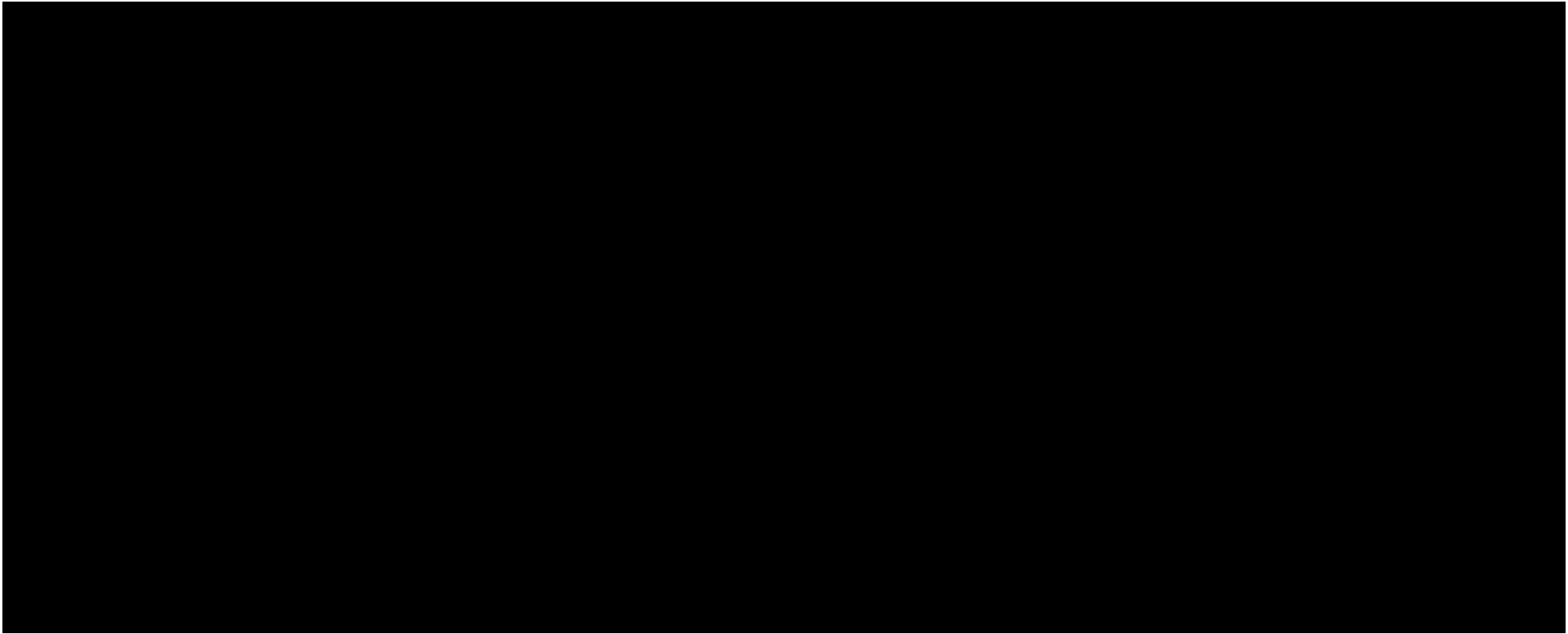


CONFIDENTIAL



CONFIDENTIAL





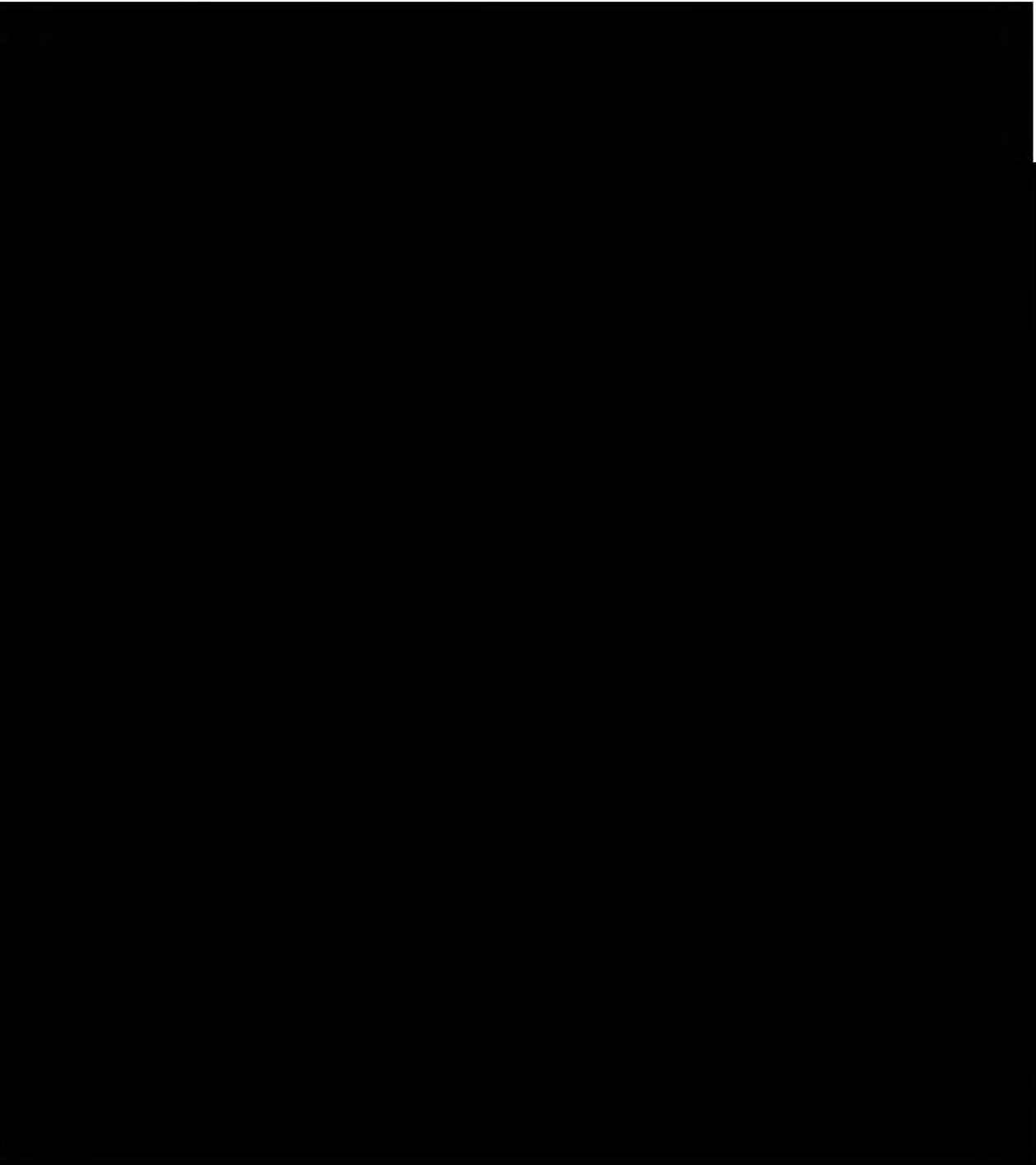
--

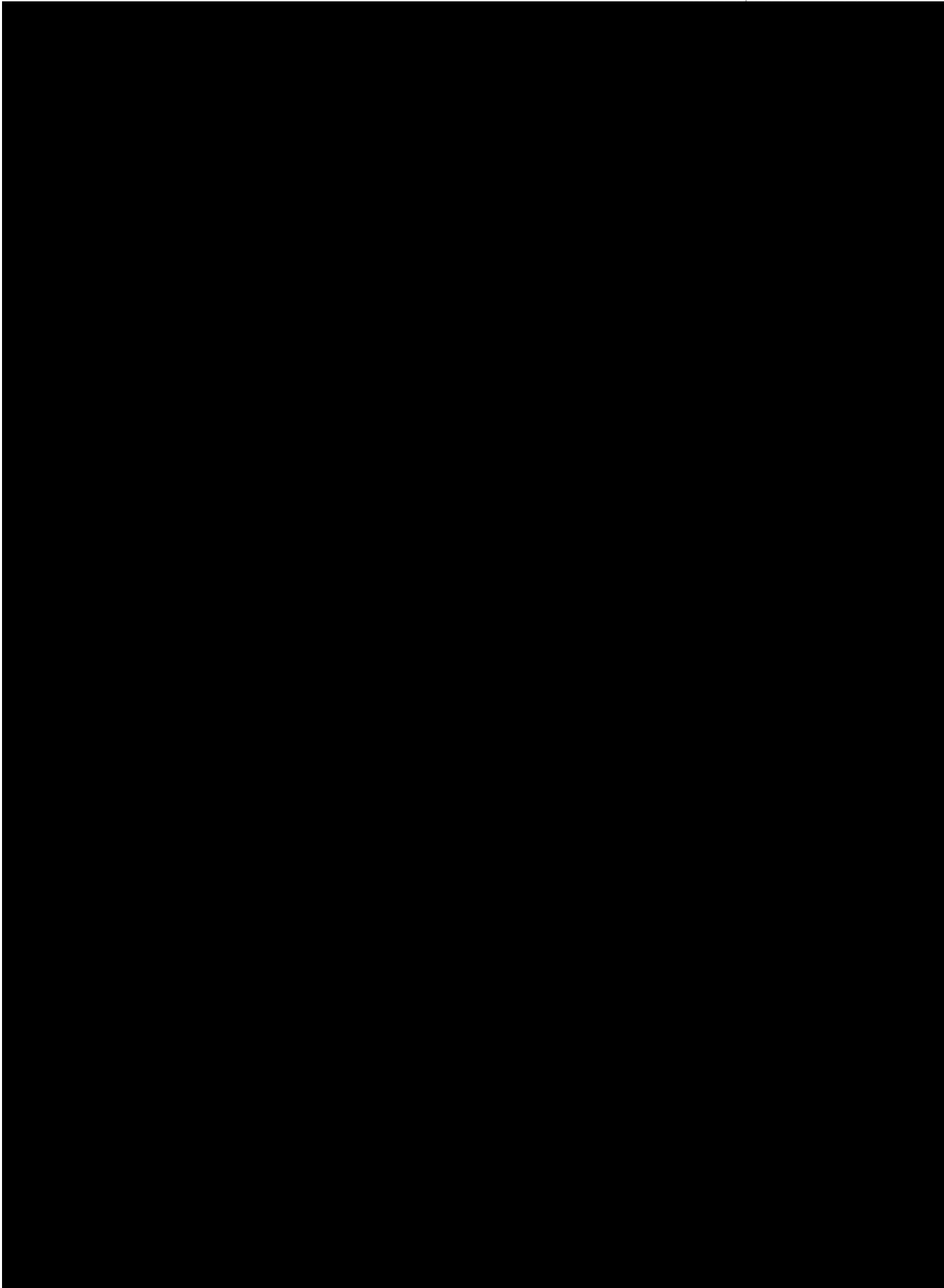
3.0 Draft Vendor Staffing Plan

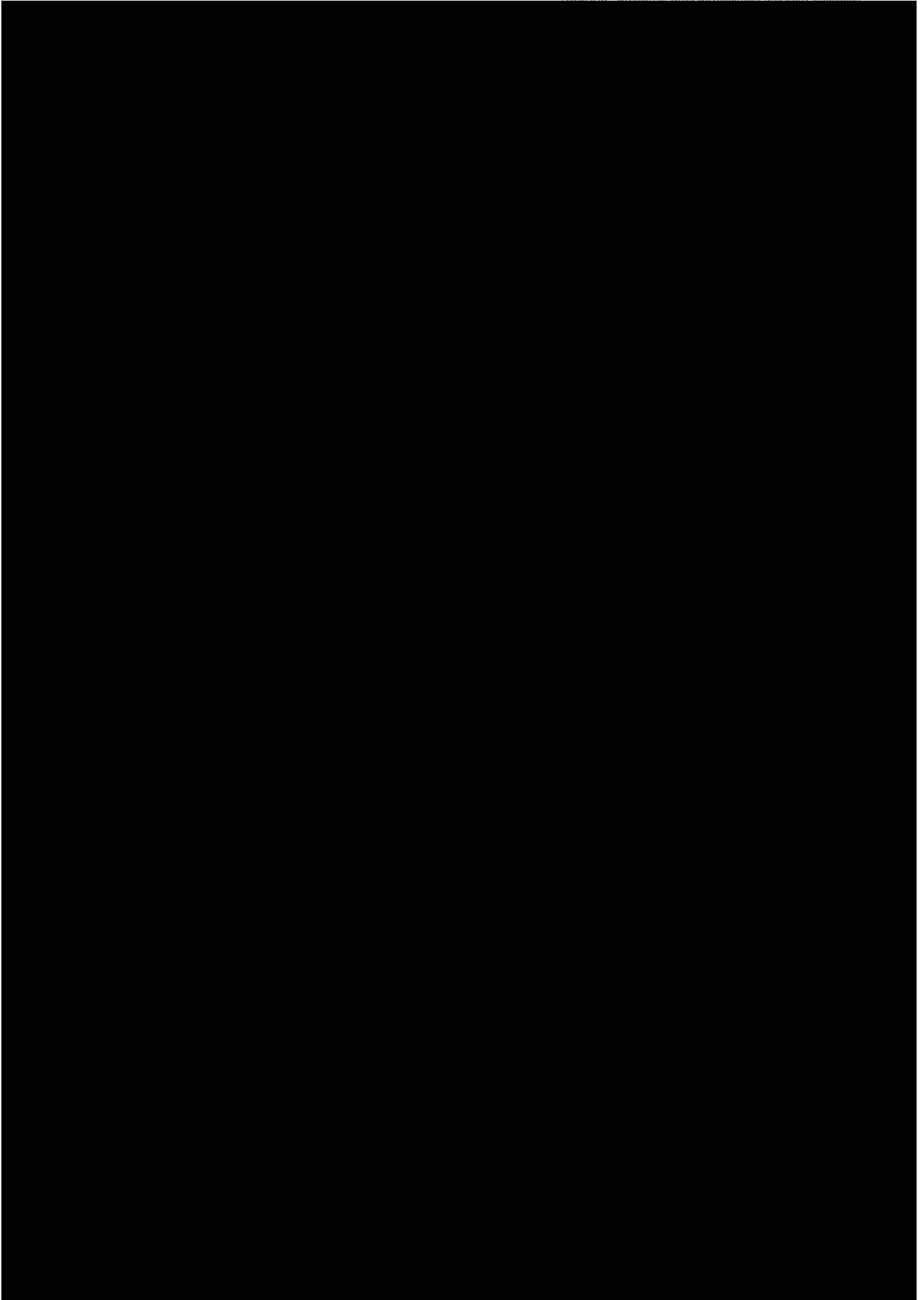
The Vendor Project Staffing Plan contains the amounts of Vendor labor resources needed to accomplish the project tasks.

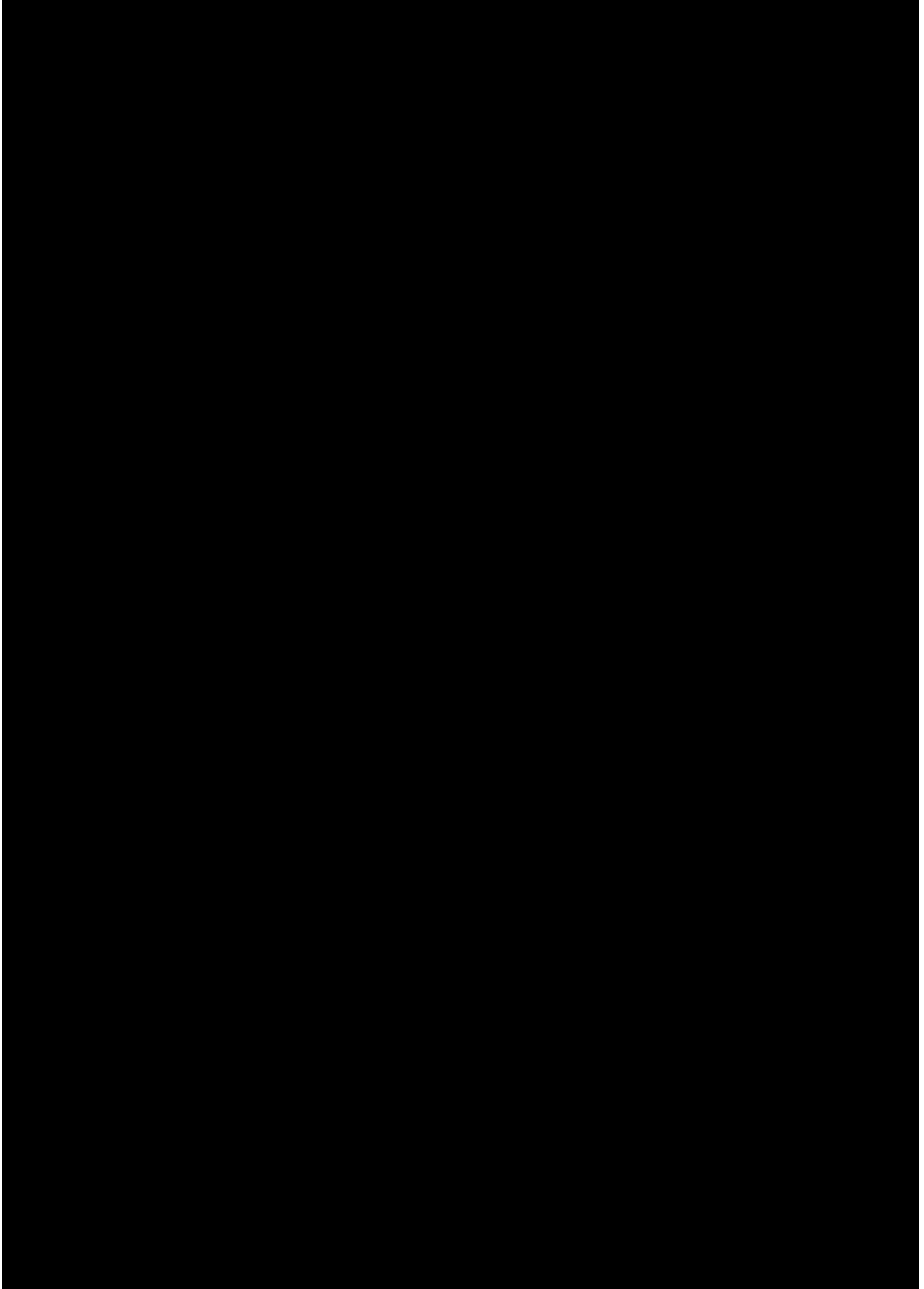
Minimum Content:

- A list of all labor resources (i.e., staffing);
 - The roles and responsibilities of all staffing resources;
 - The percentage of each staffing resource's time needed in each phase/stage;
 - Specification of how long each resource will be needed for each stage of the project;
 - Definition of skills required of each staffing resource; and
 - Plan for resource turnover.
-



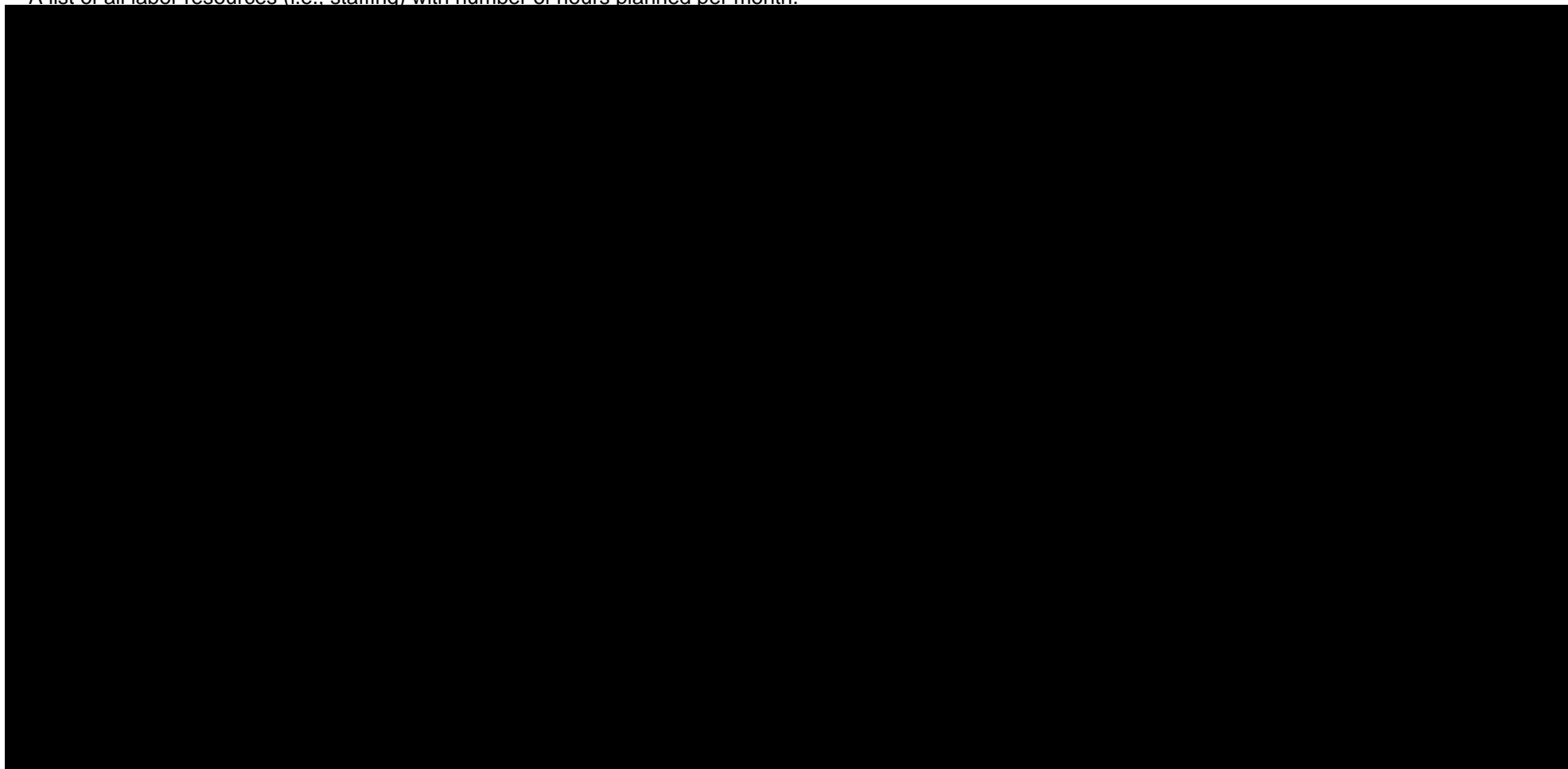


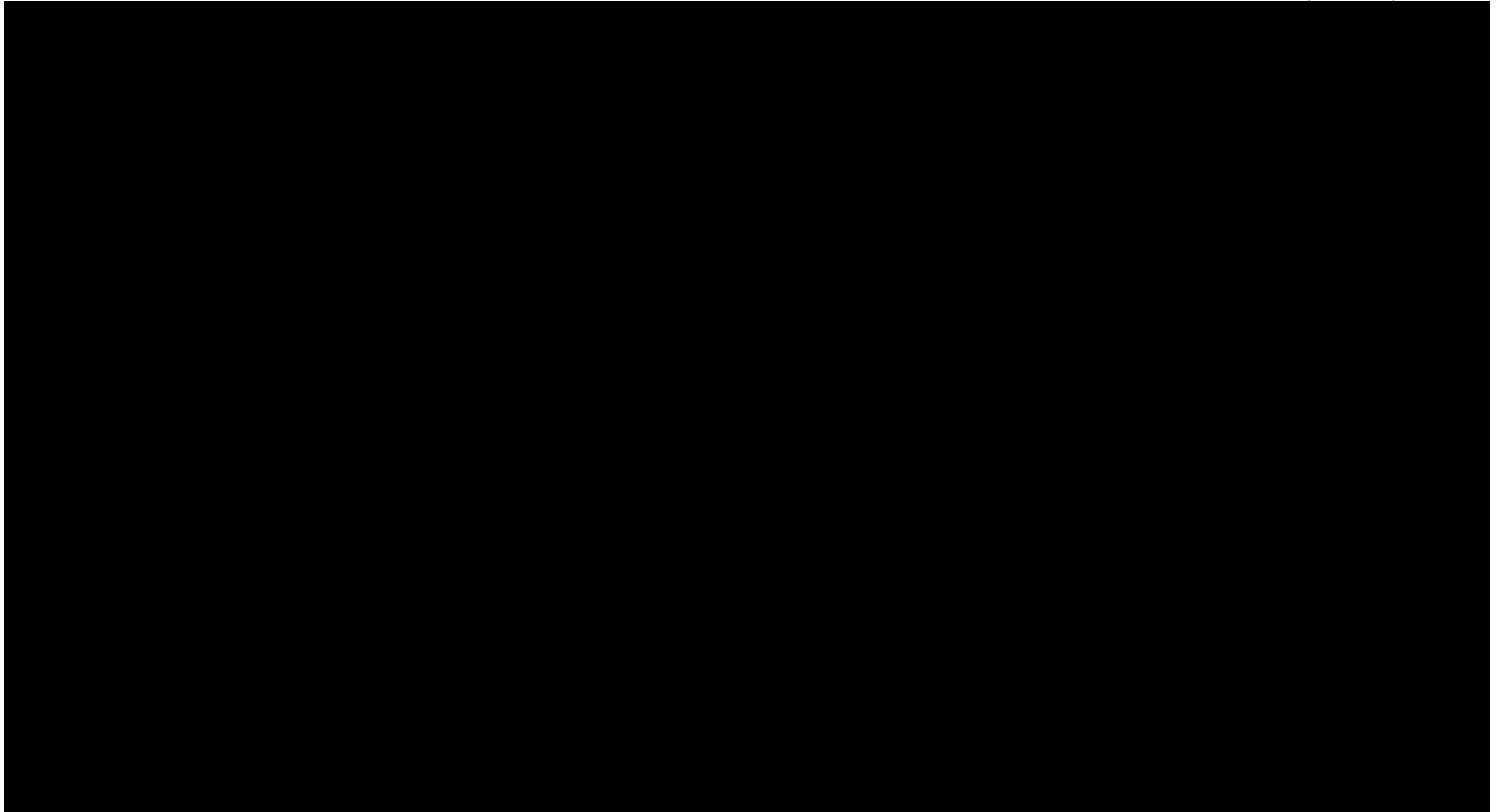


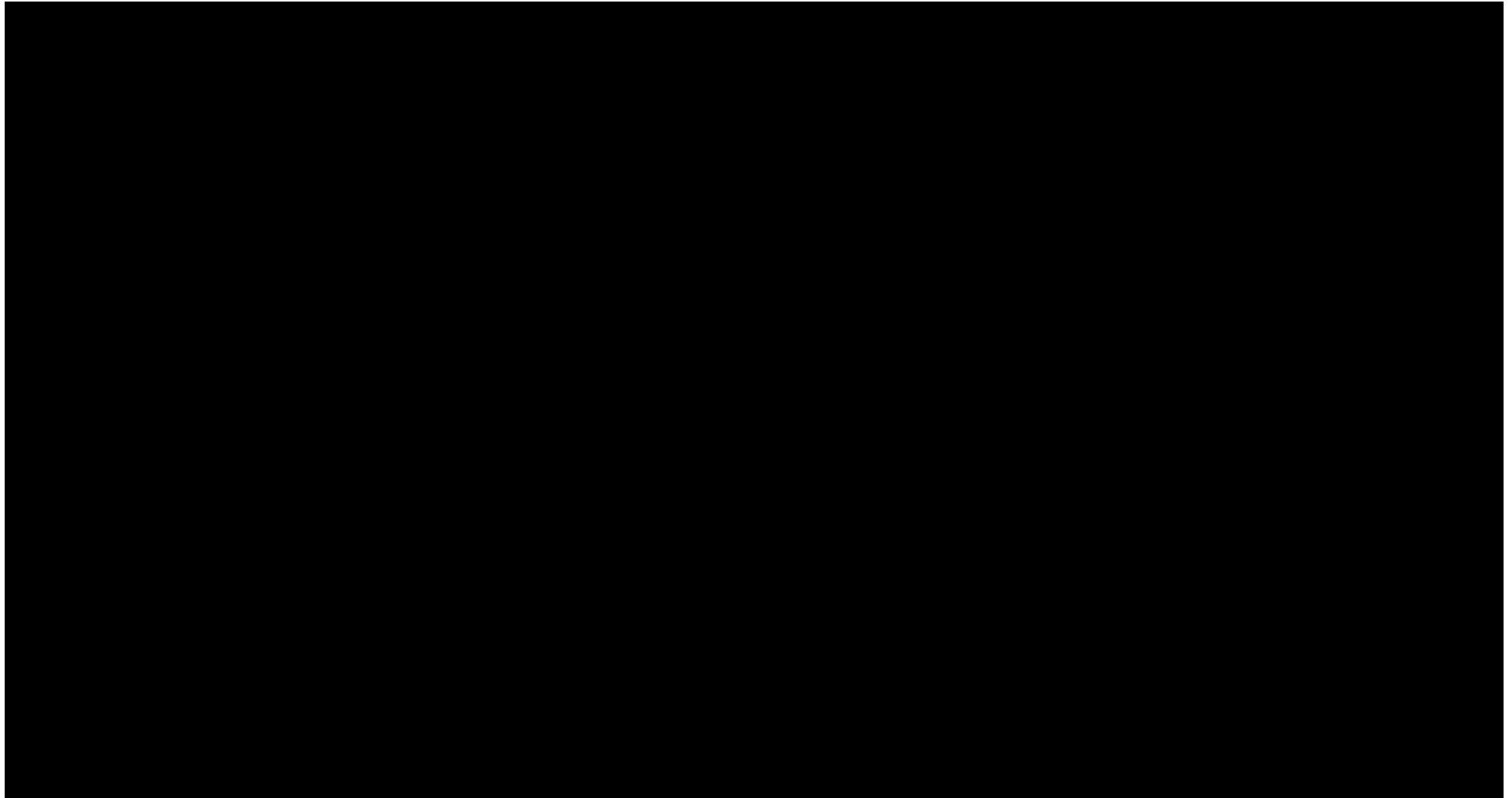


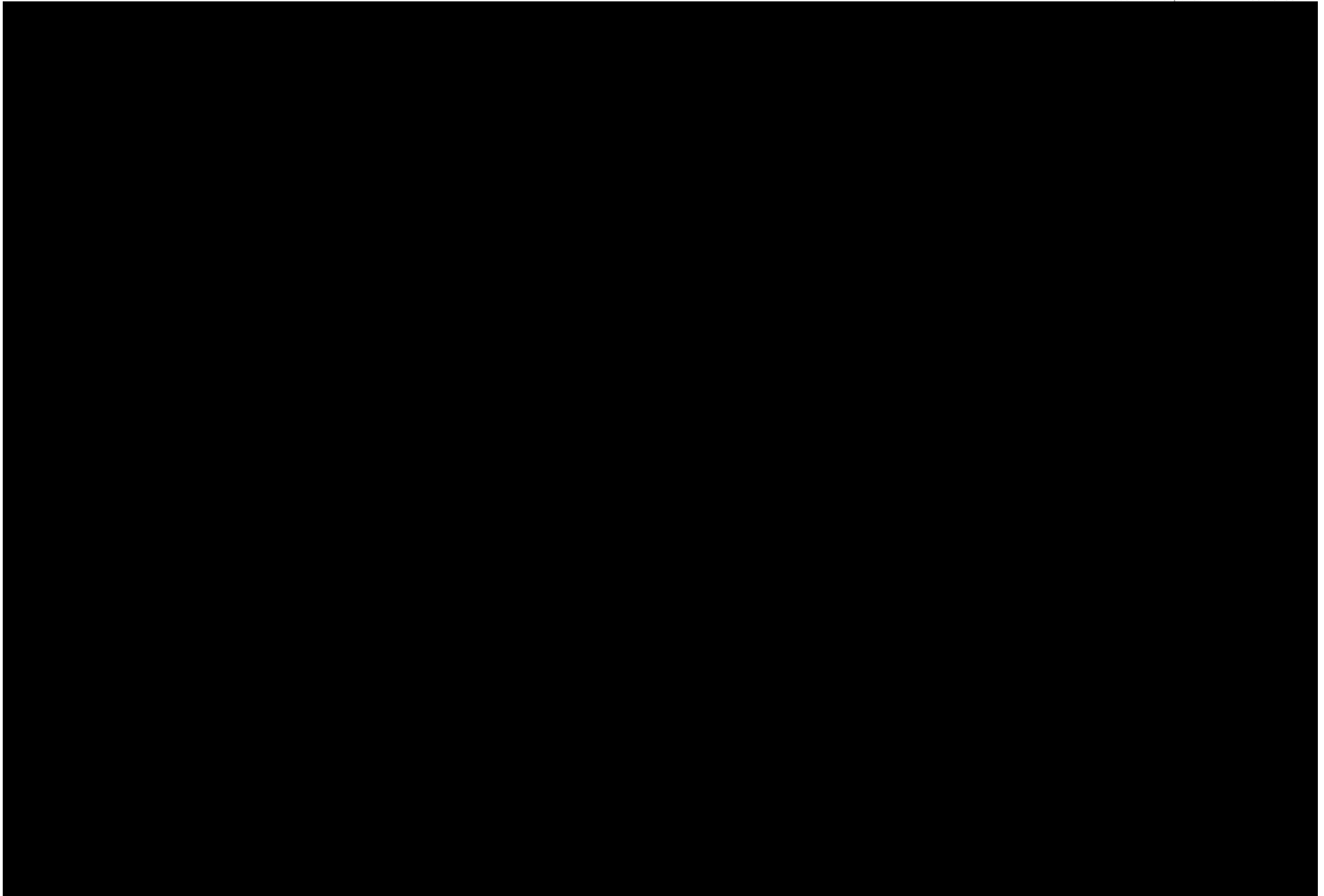
A. Staffing Plan

A list of all labor resources (i.e., staffing) with number of hours planned per month.



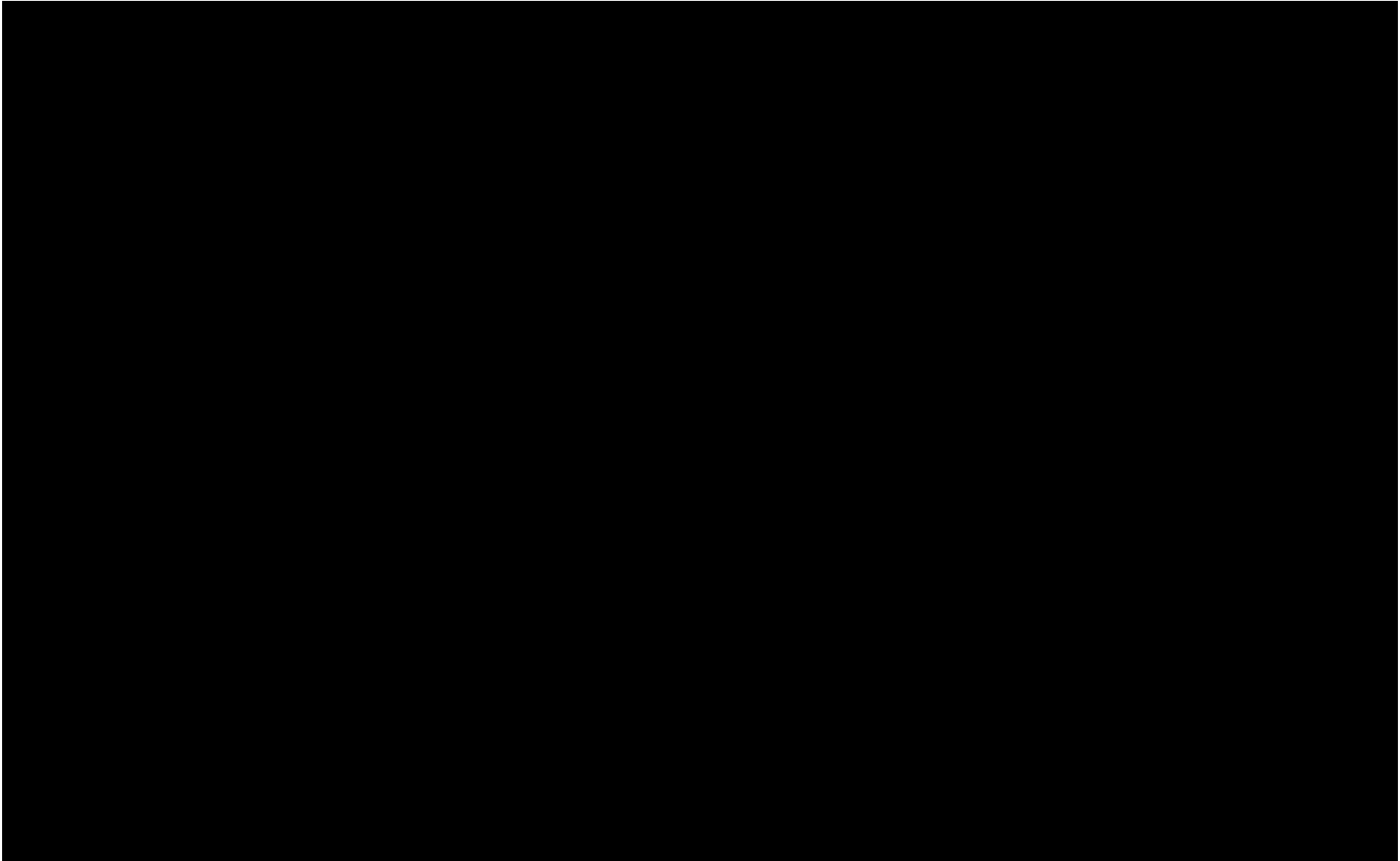


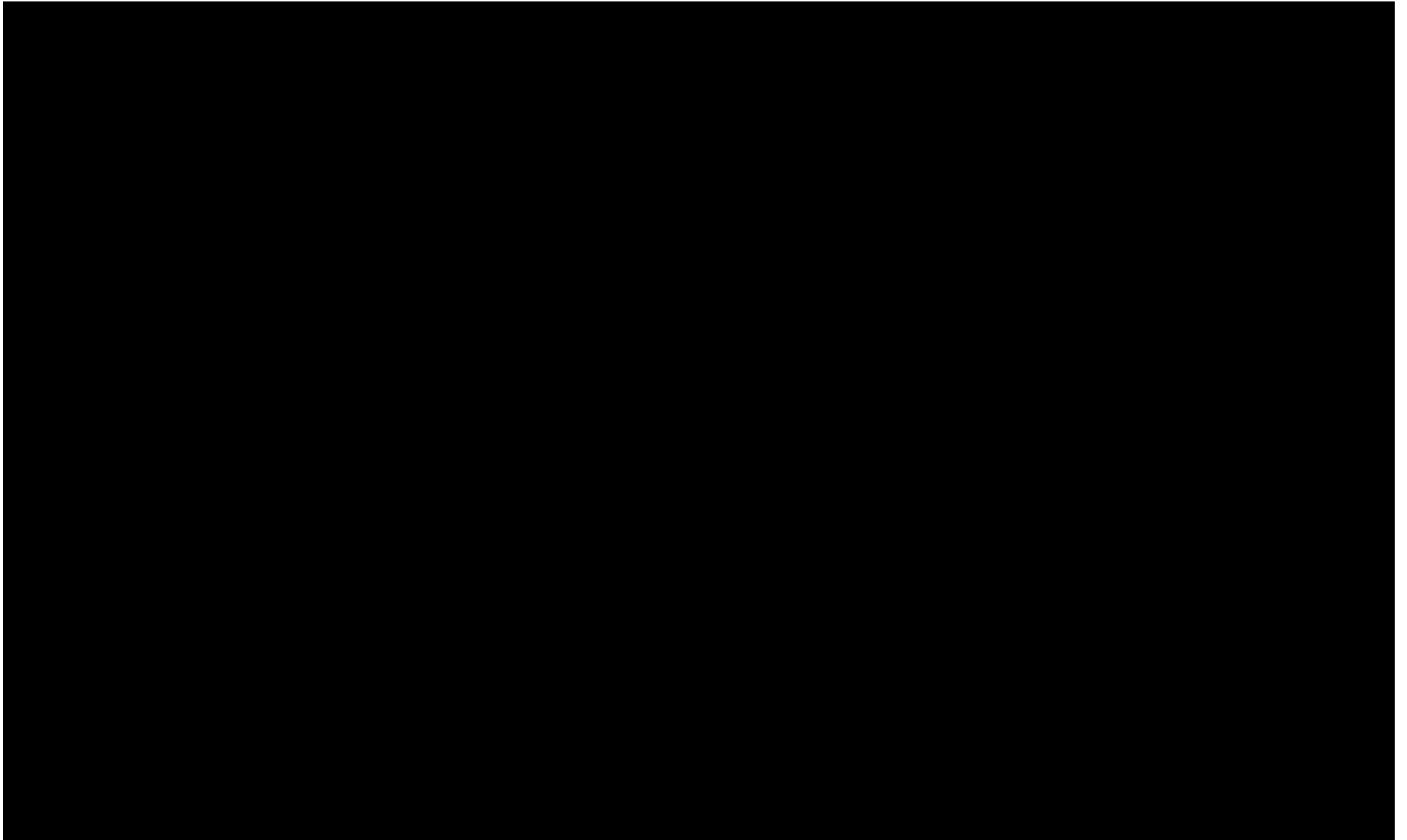


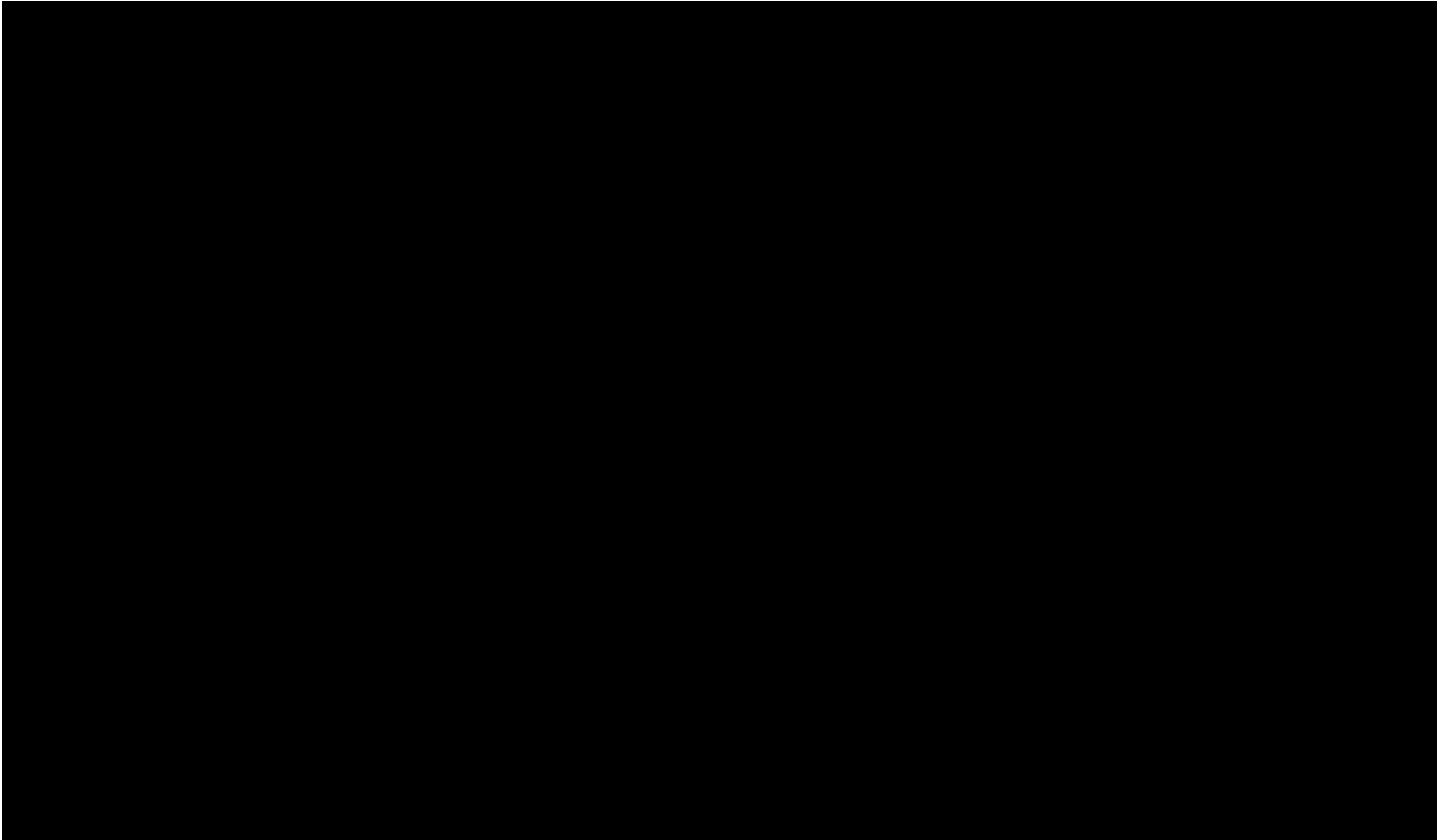


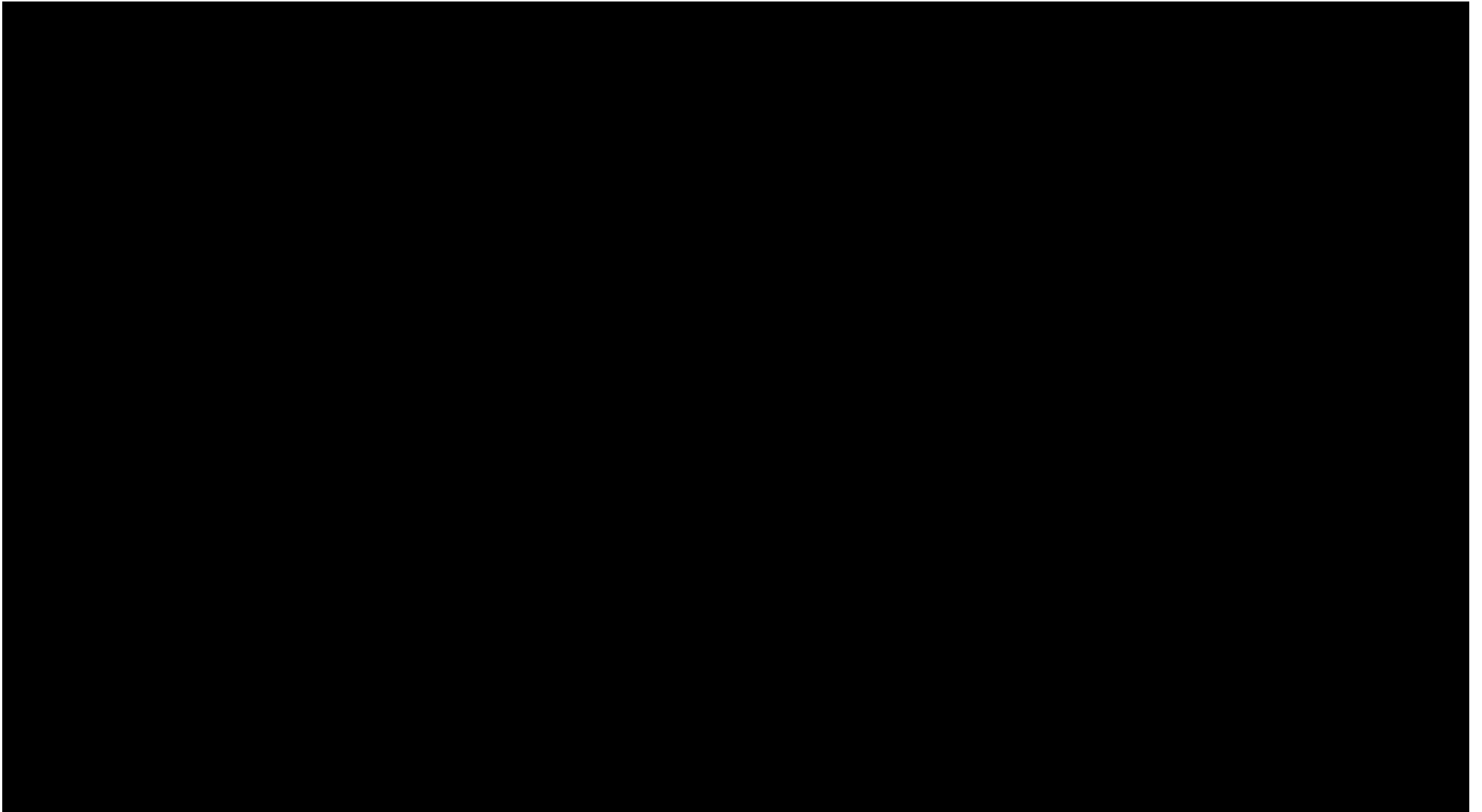
B. Staffing Plan by phase/stage

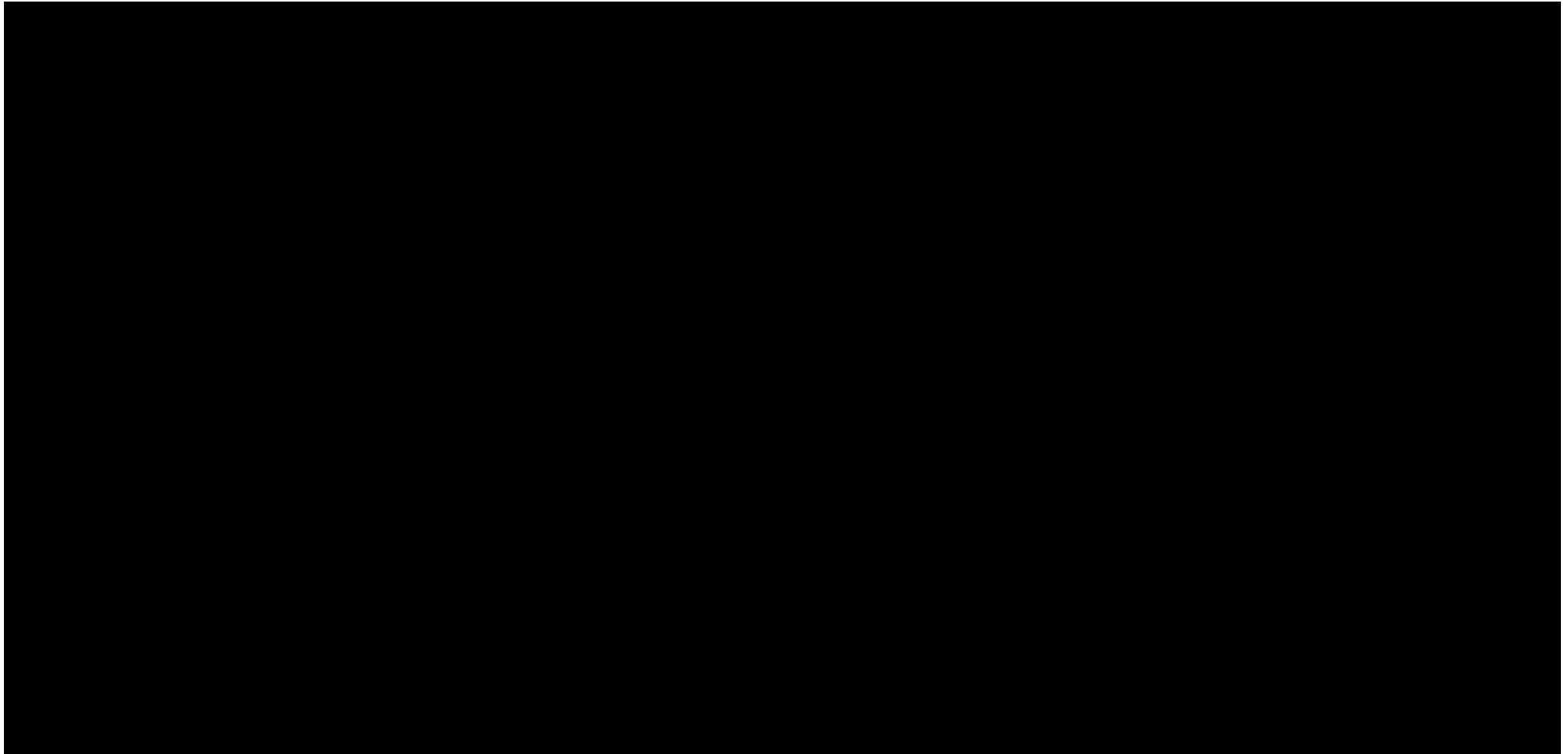
In the subsequent section, we dive into the critical aspects of our project staffing: the percentage of each staffing resource's time in each phase/stage, and



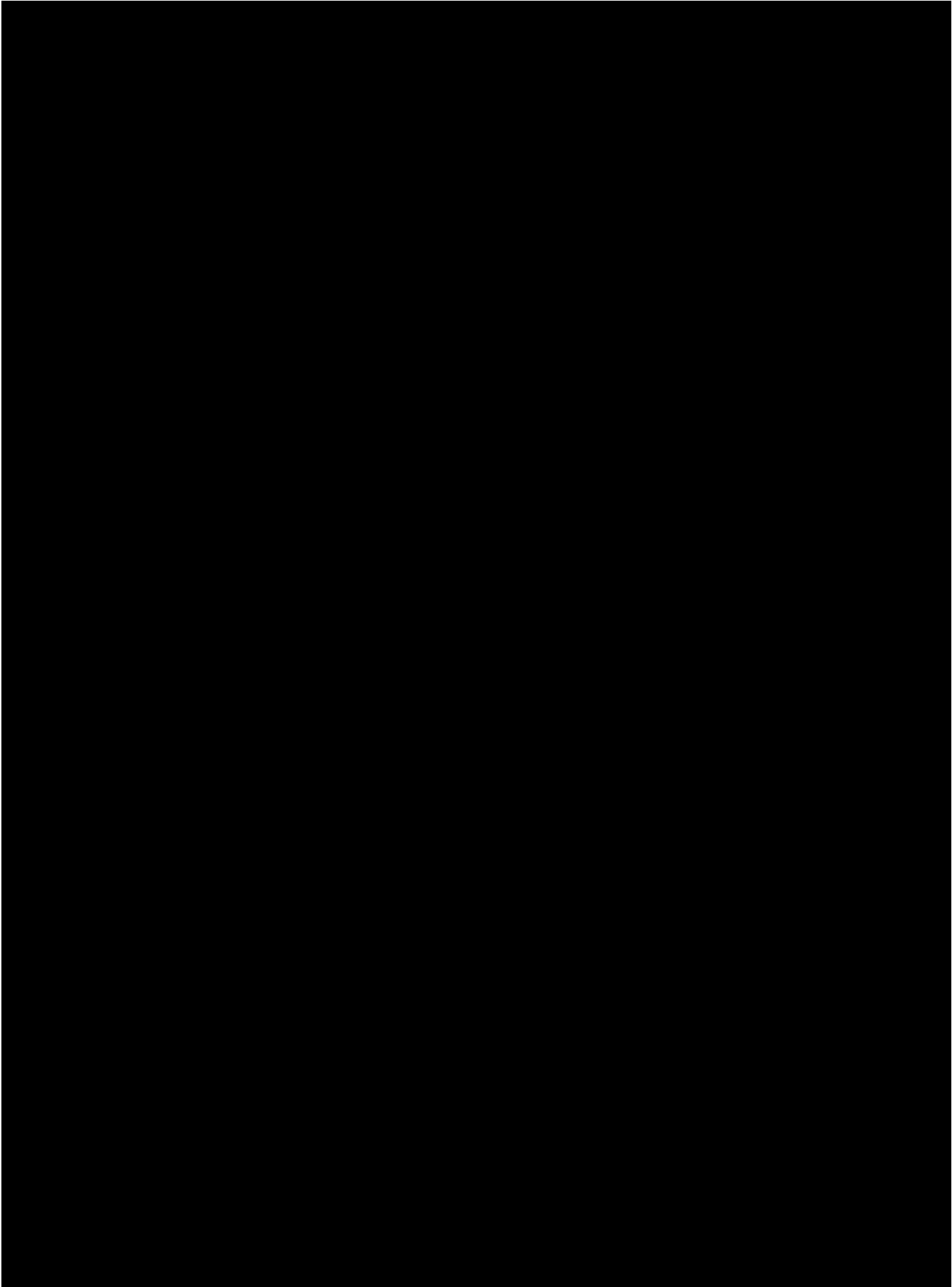


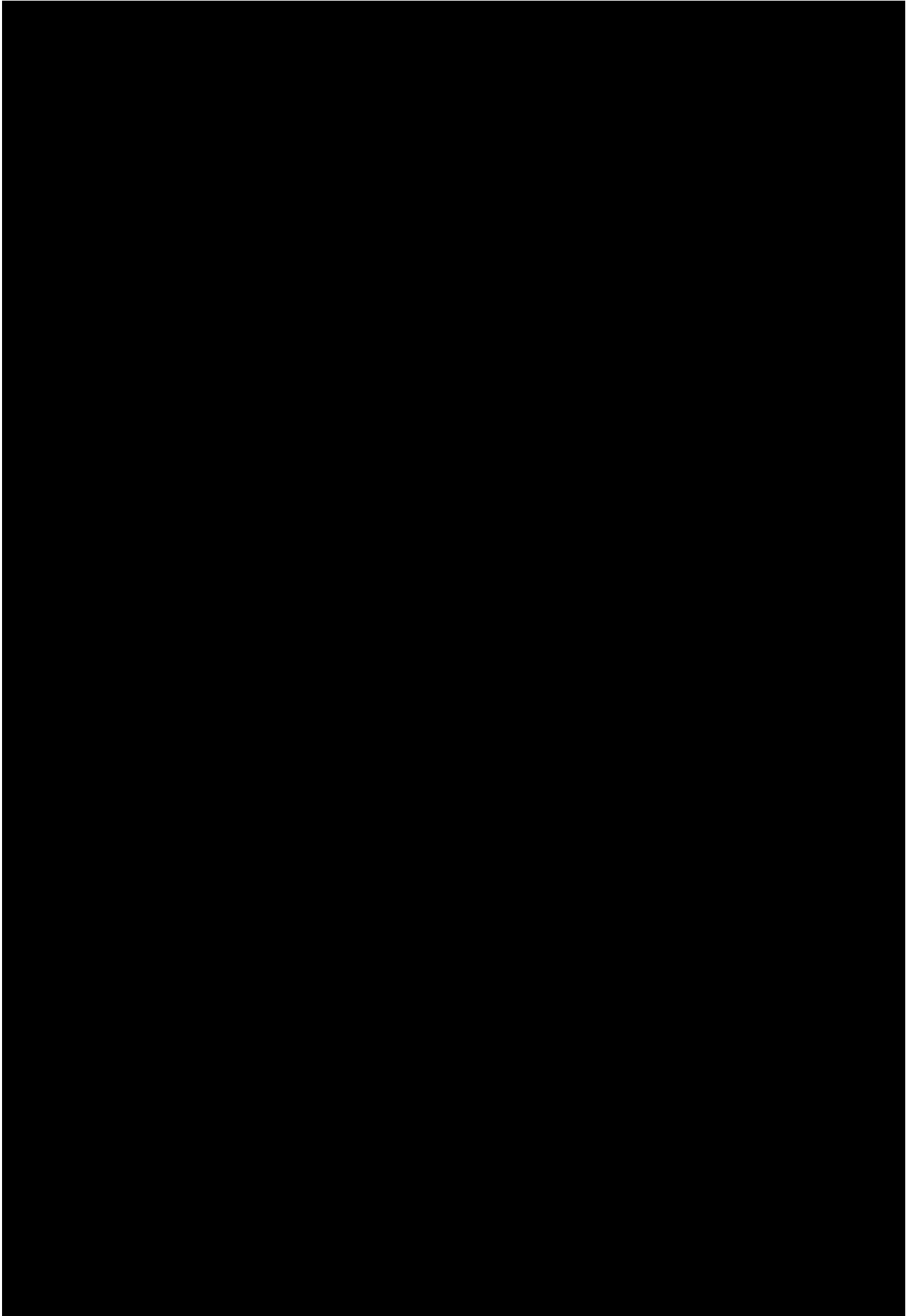


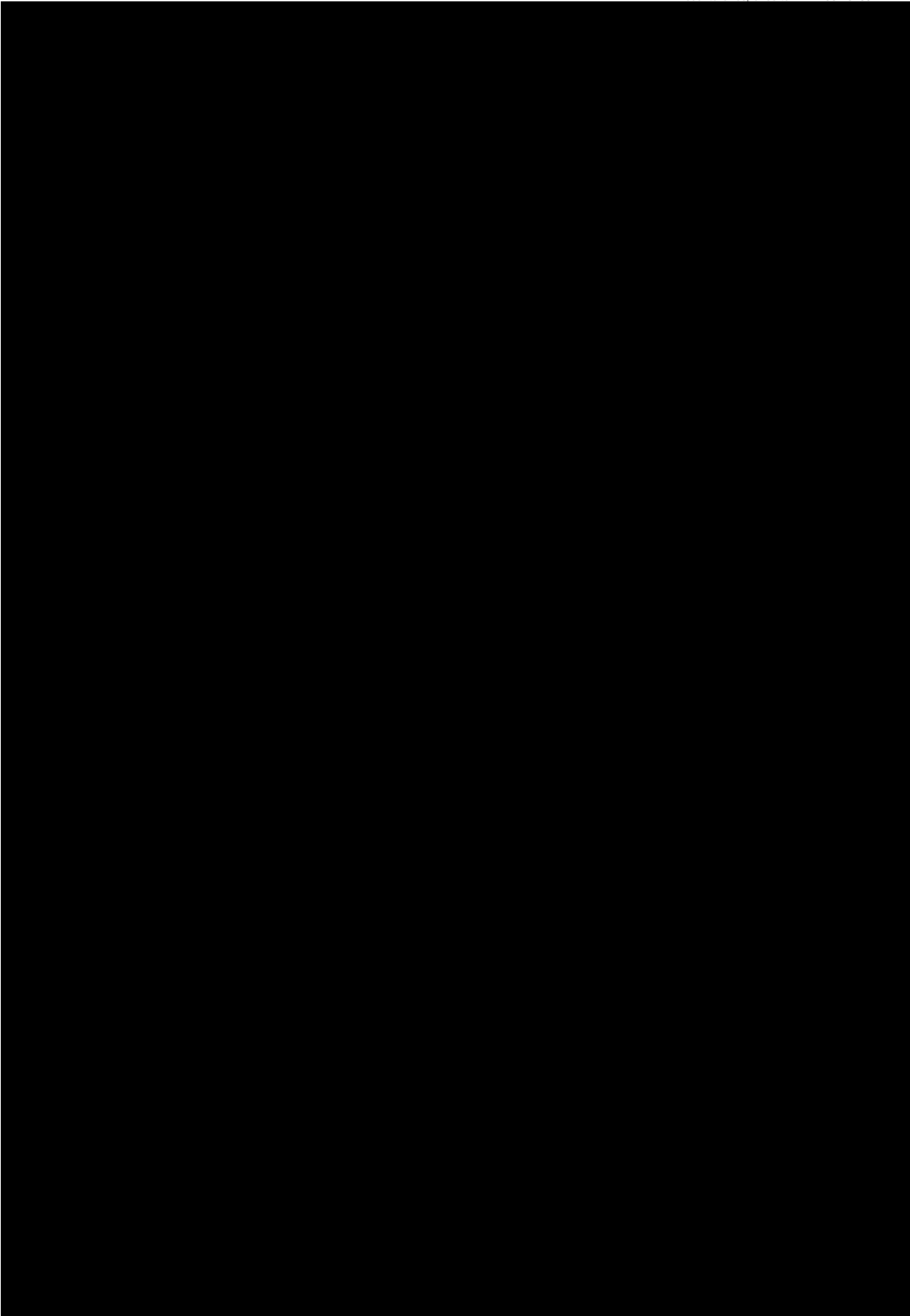


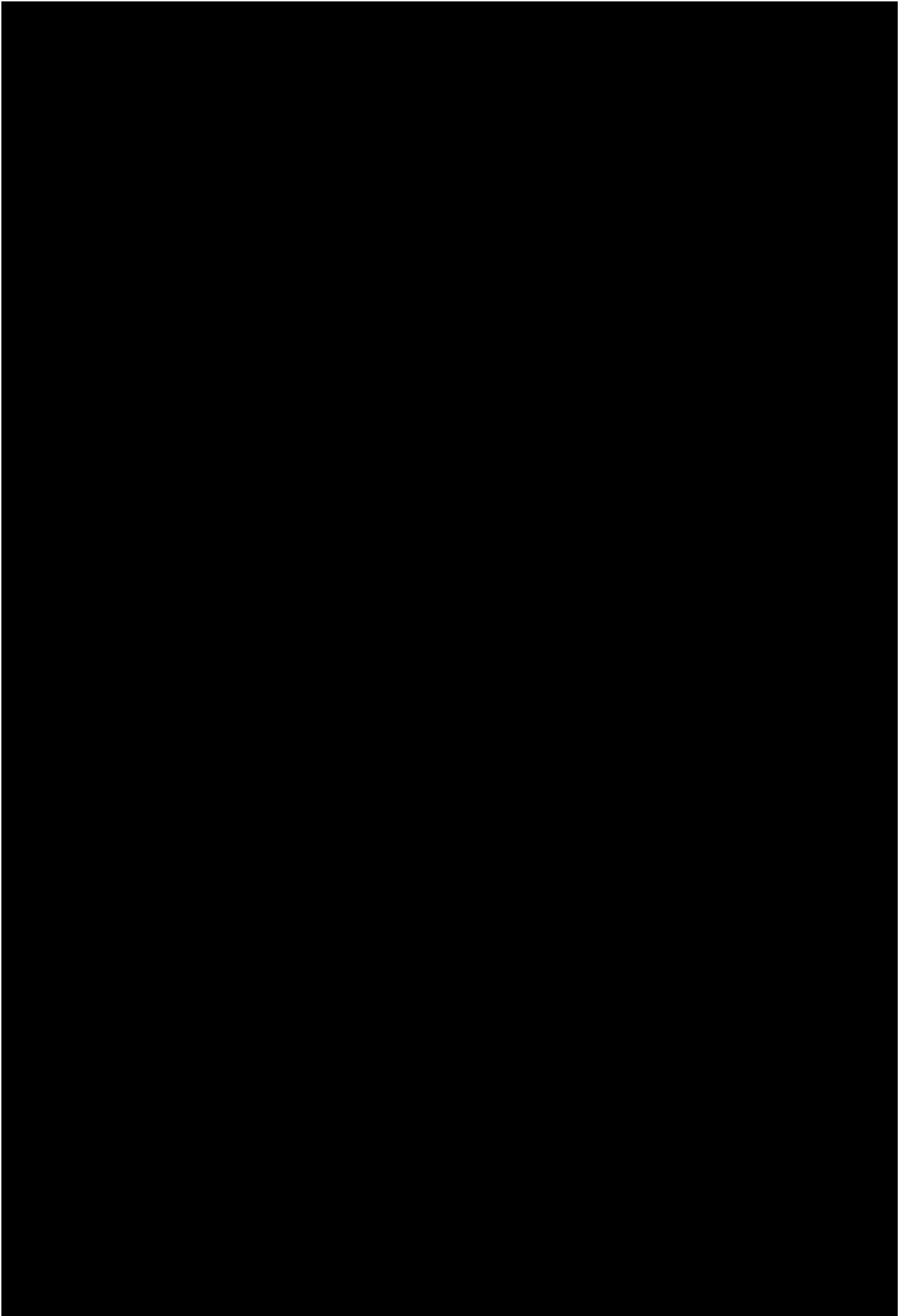


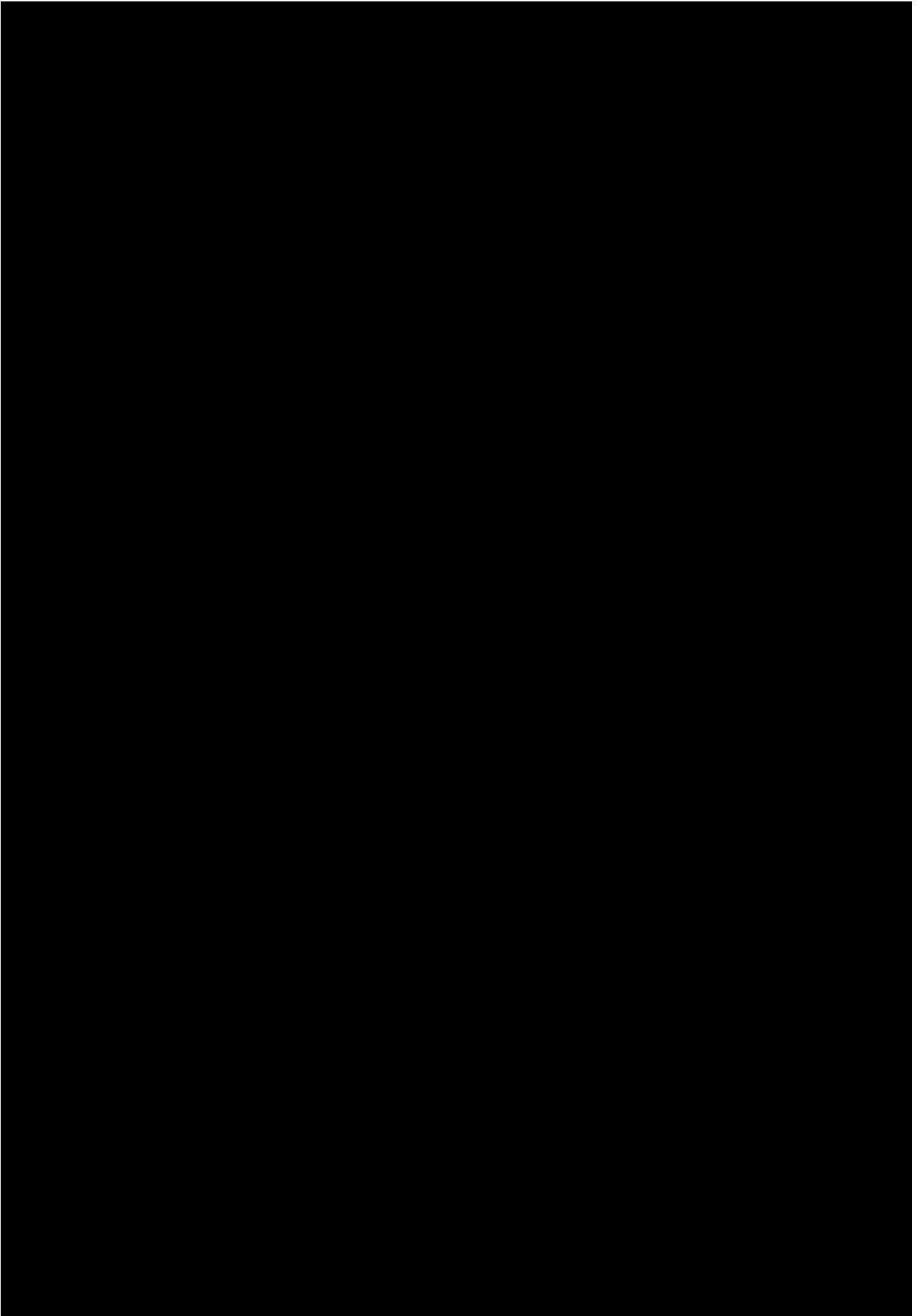
Completion of Project Deliverables will follow the process described in our response to the Draft Project Management Plan, section G. Project Deliverables, and the Draft Schedule. The table below depicts Responsible Accountable Consulted and Informed (RACI) matrix between DCDEE and Accenture.

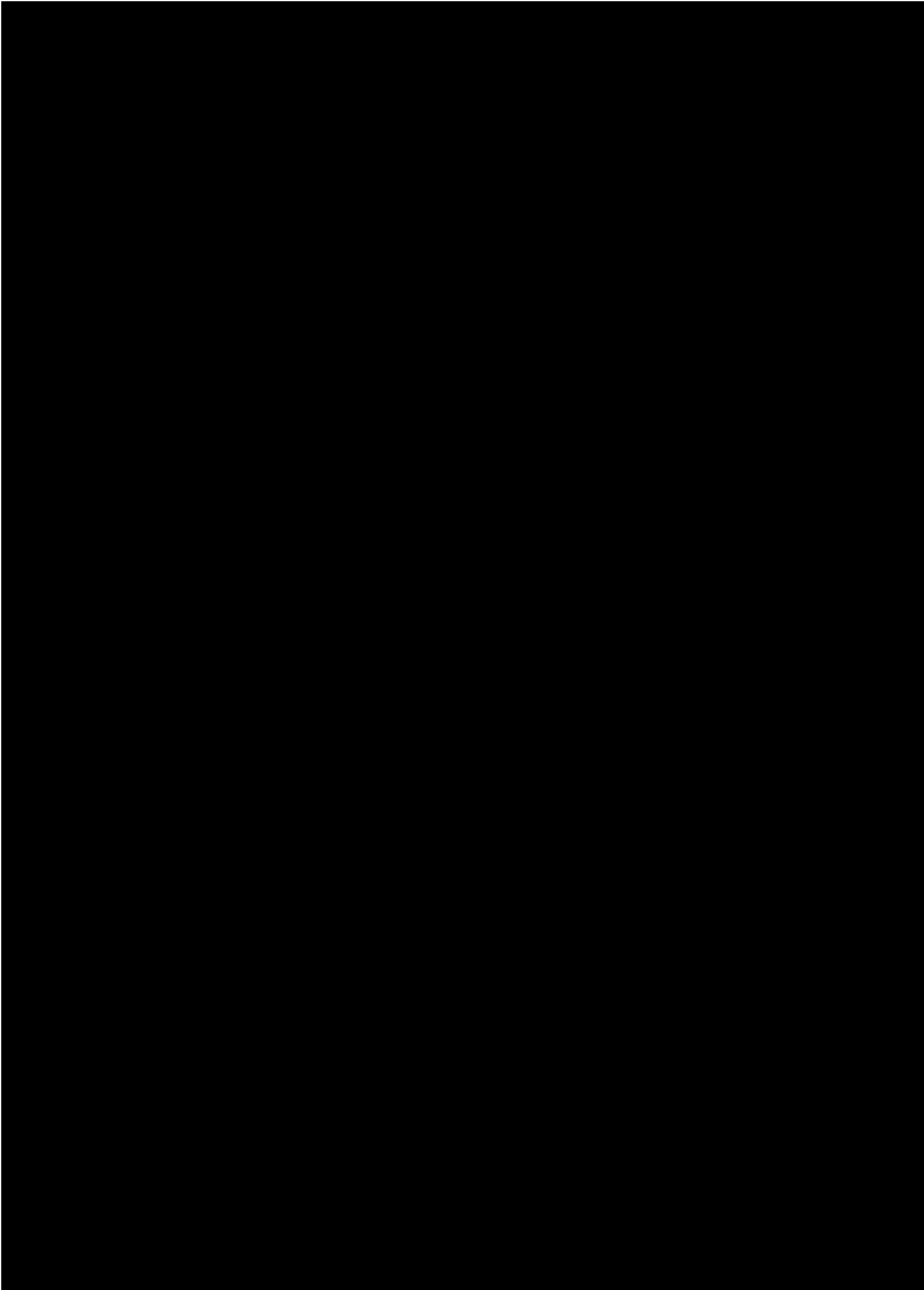






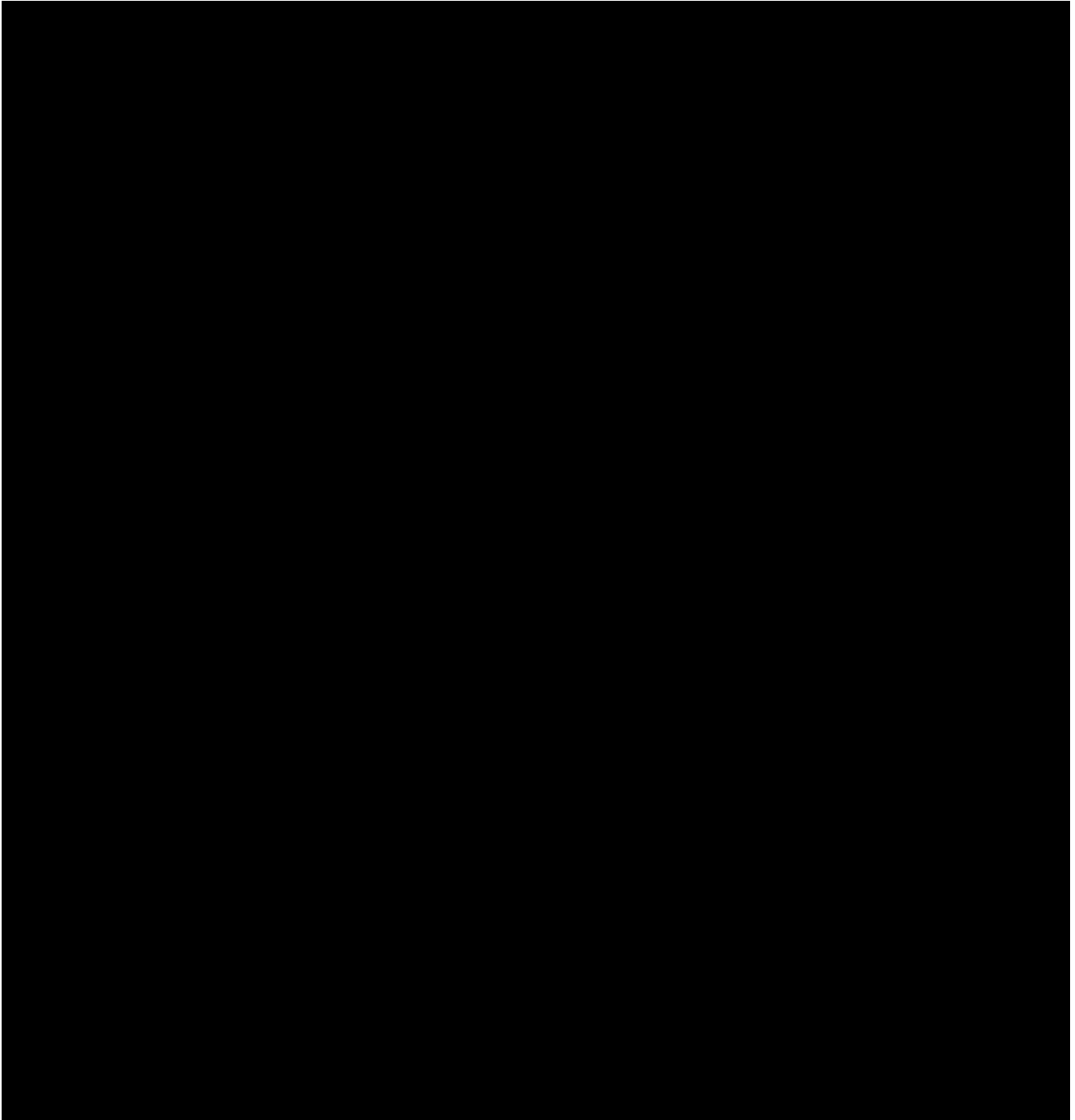


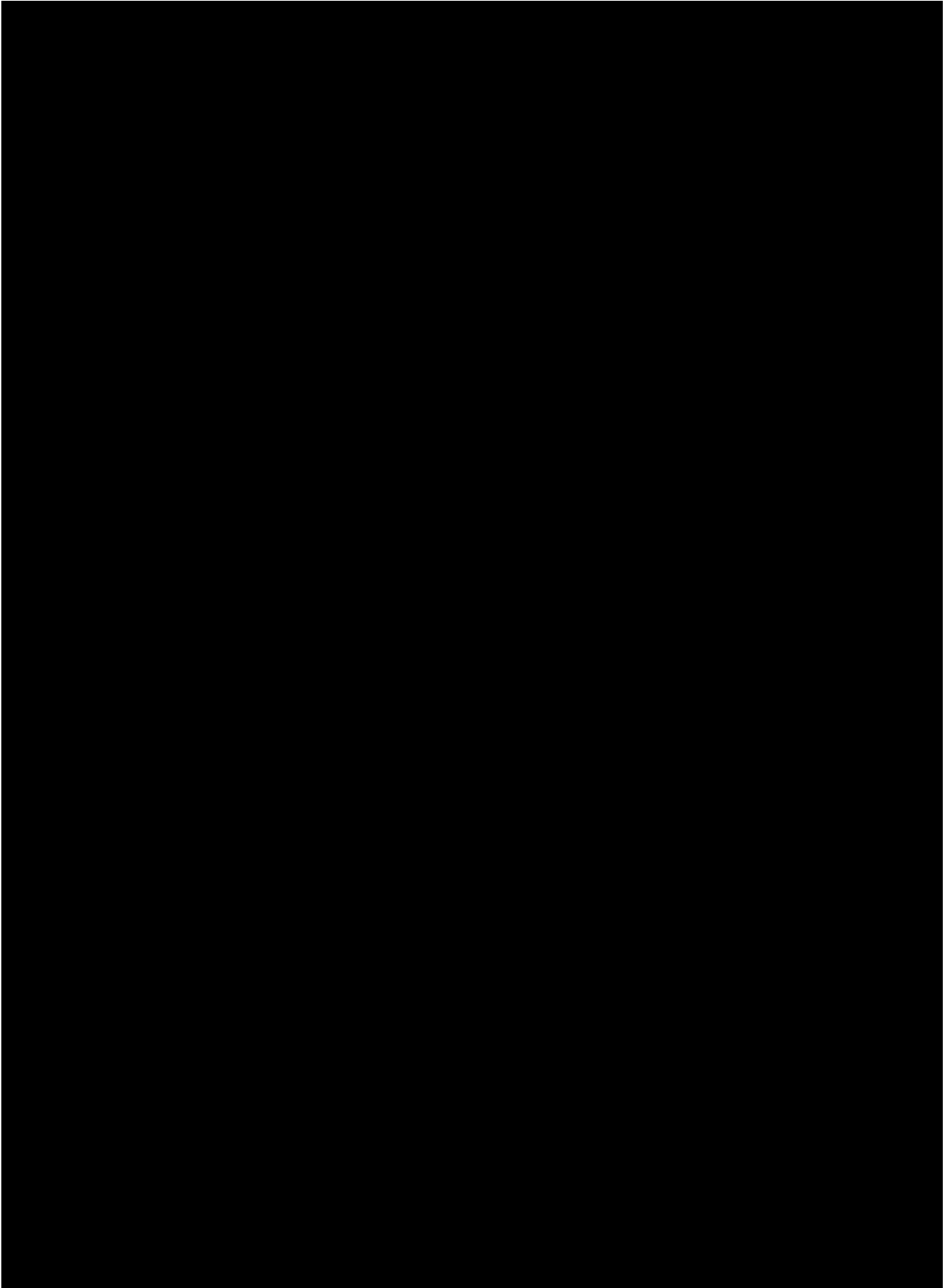


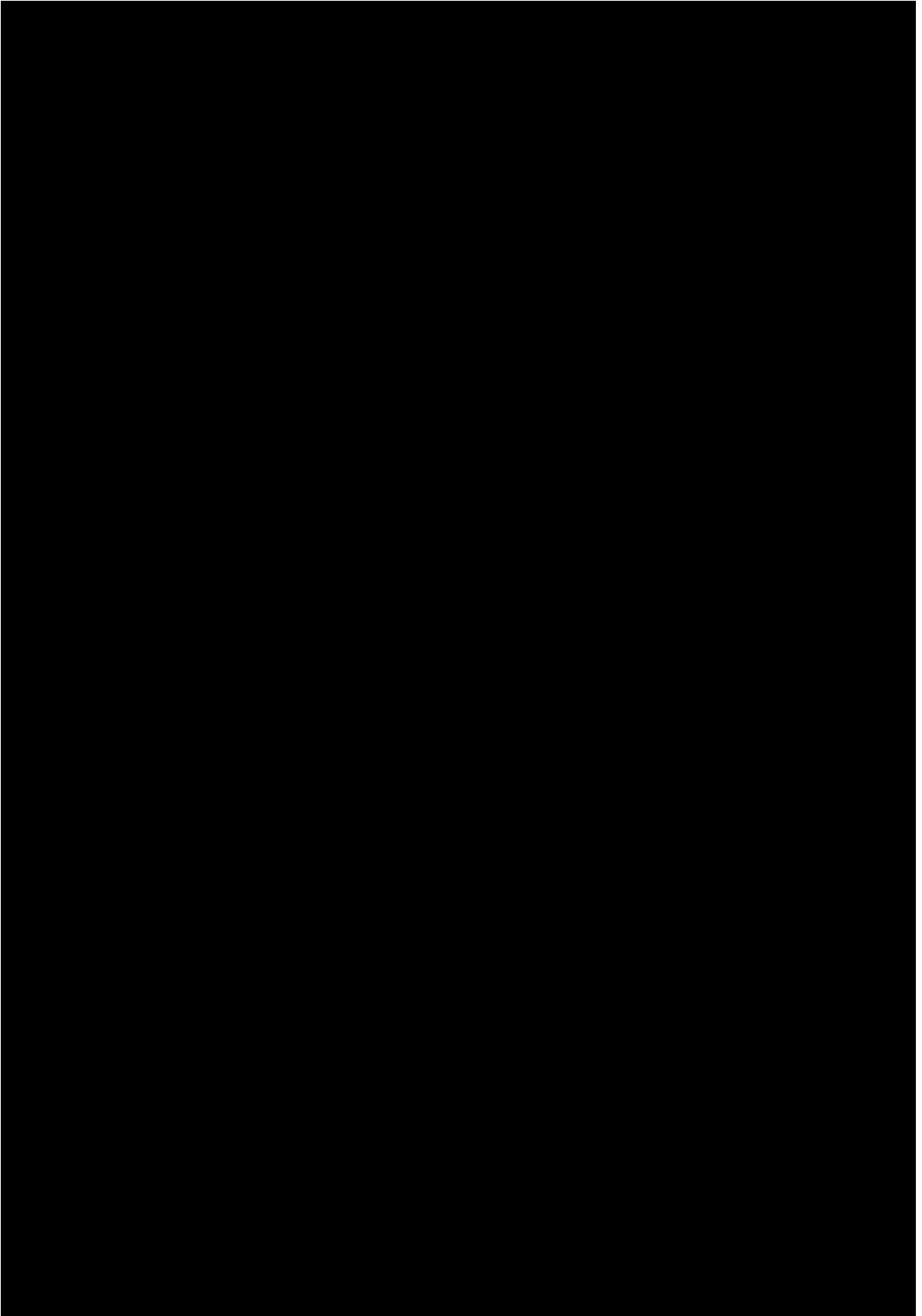


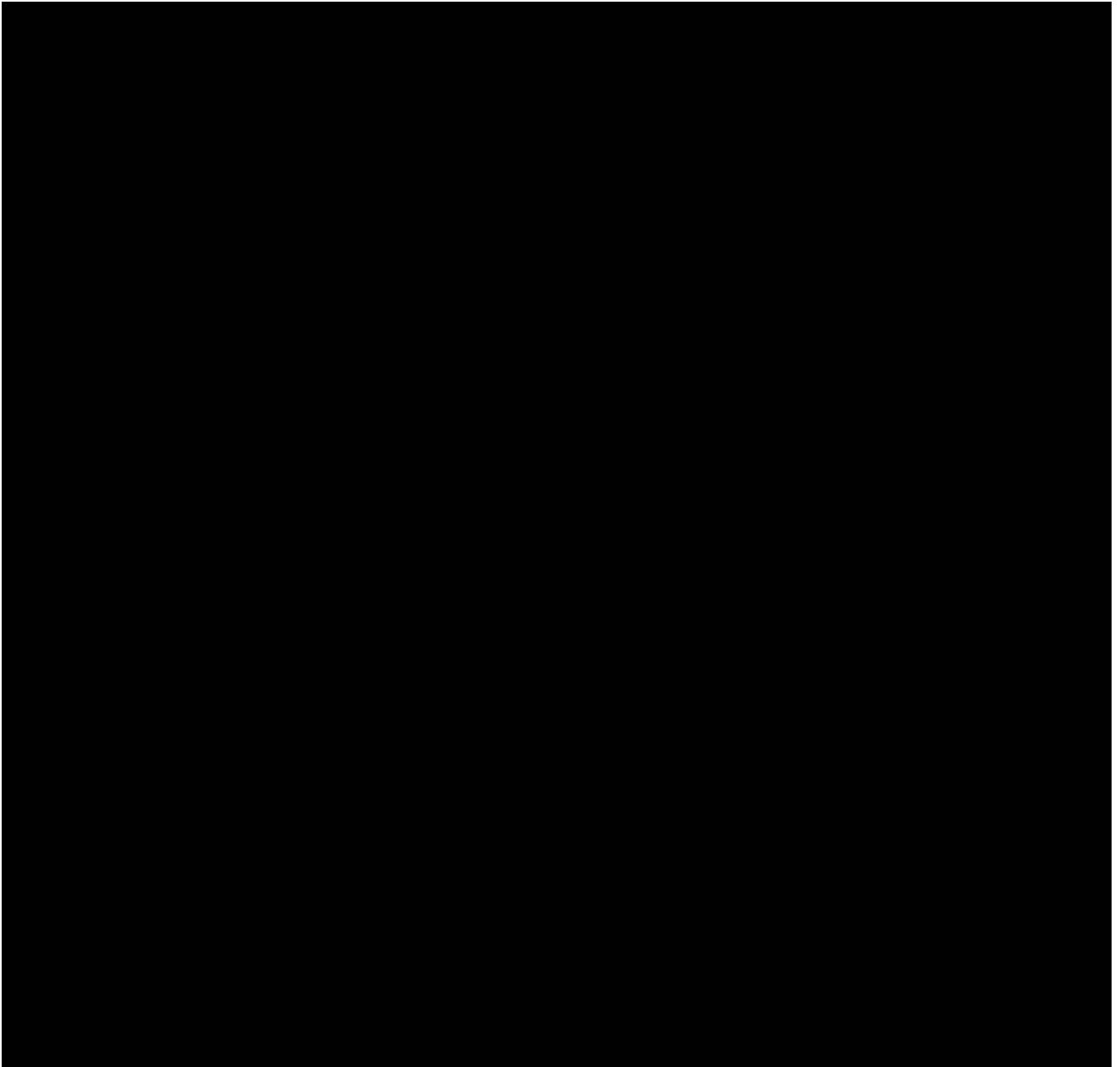


NCDHHS Roles and Responsibilities



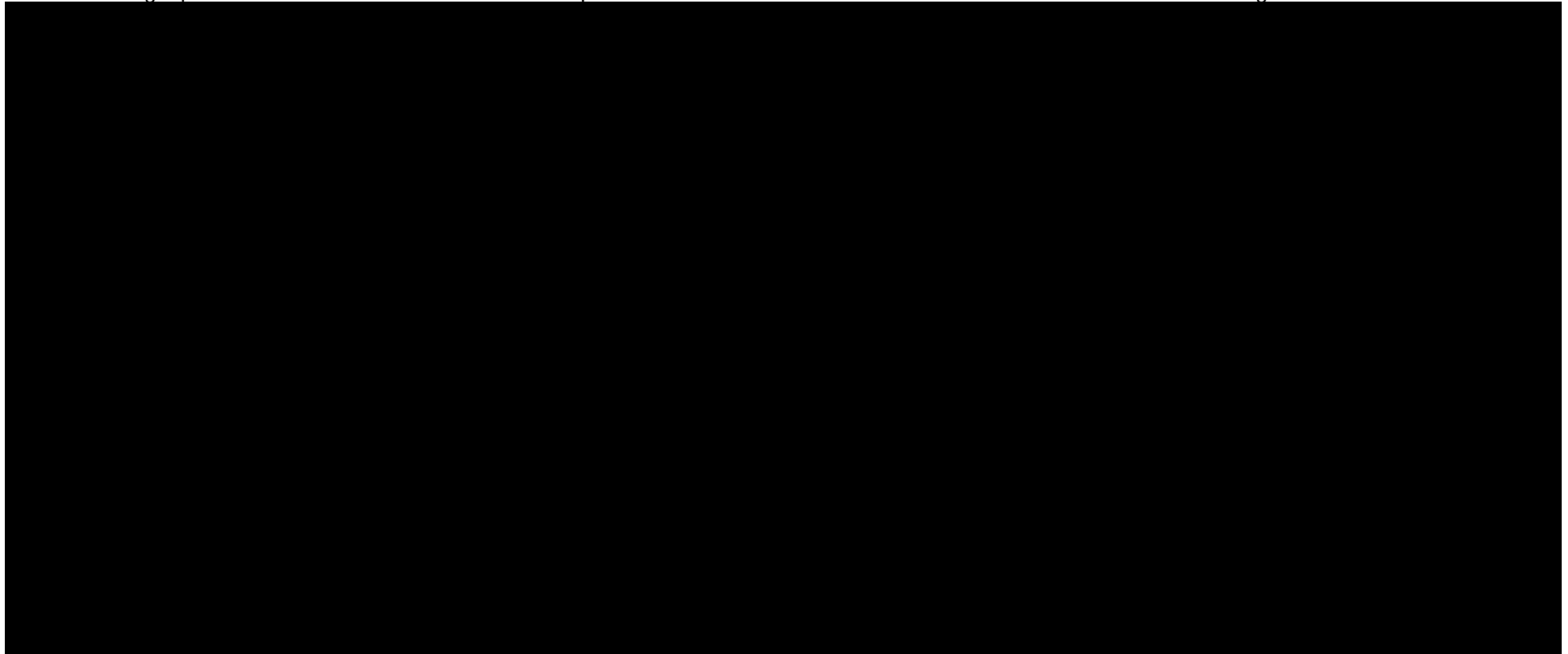






D. Organization Chart

The following represents the resources identified for the implementation of NC-PROCEED this includes Accenture and State staffing.

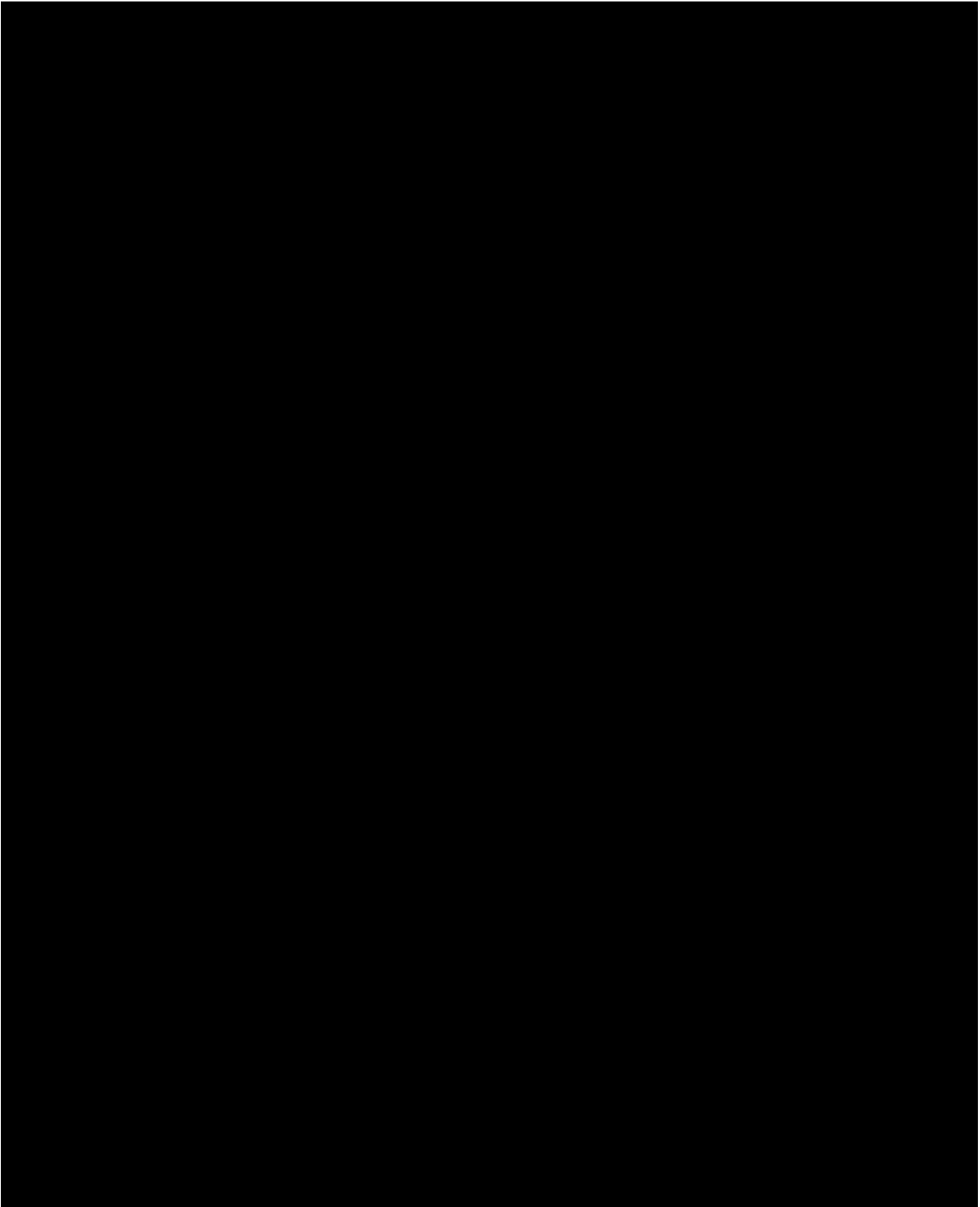


E. Skills required for NCDHHS staffing resource

See Section B. Roles and Responsibilities for a detailed view of skills required per NCDHHS role.

F. Plan for resource turnover

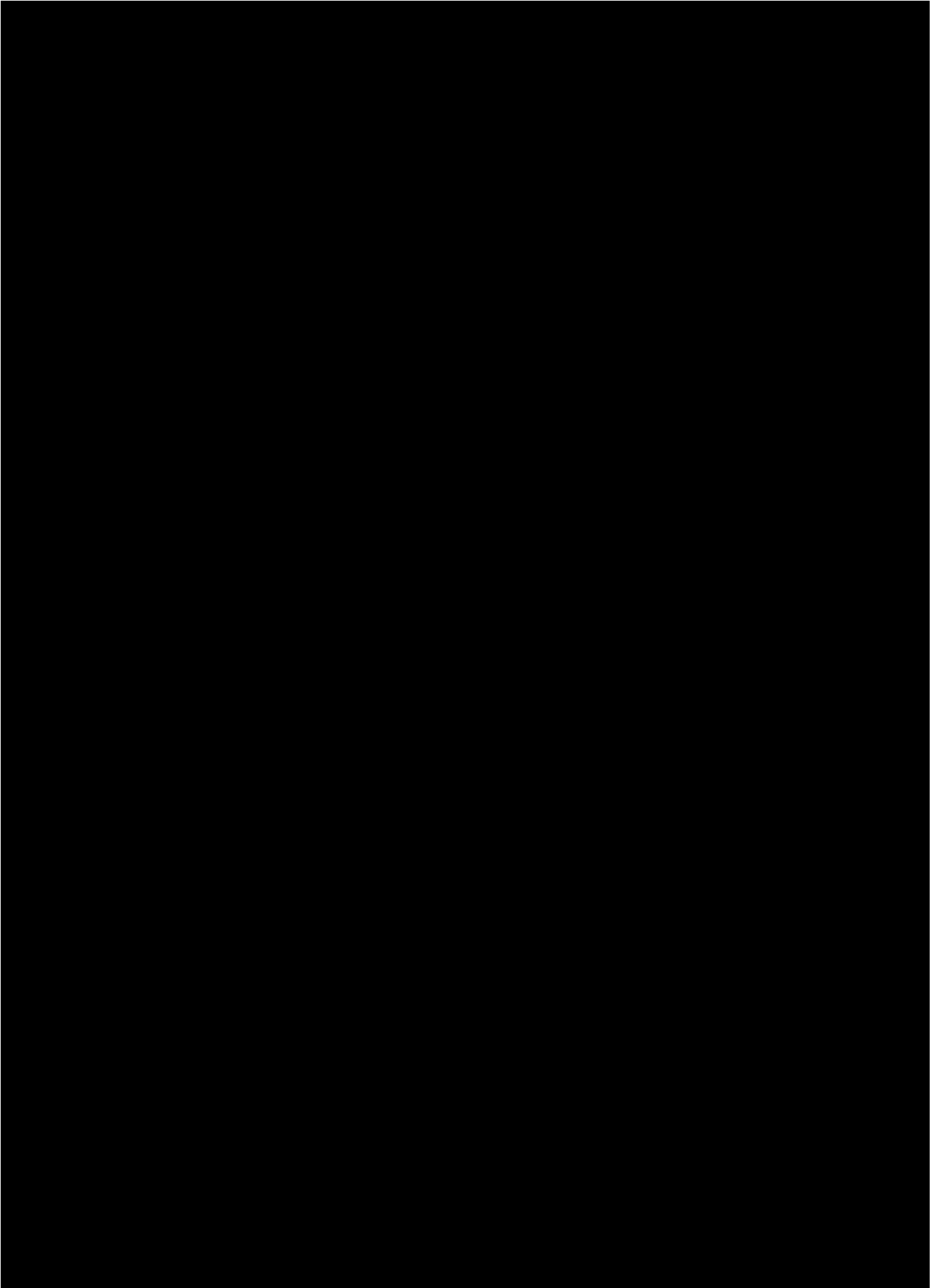


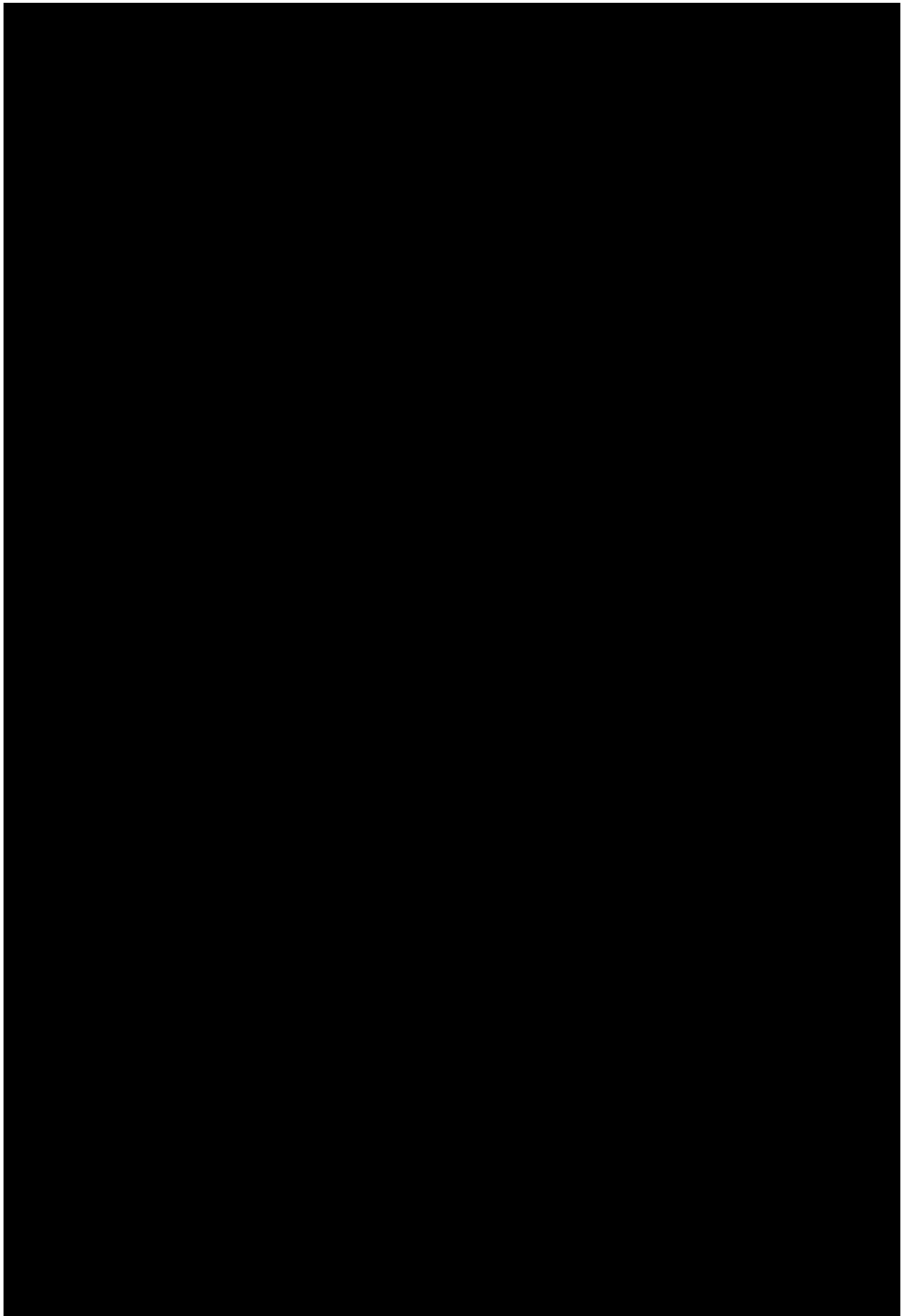


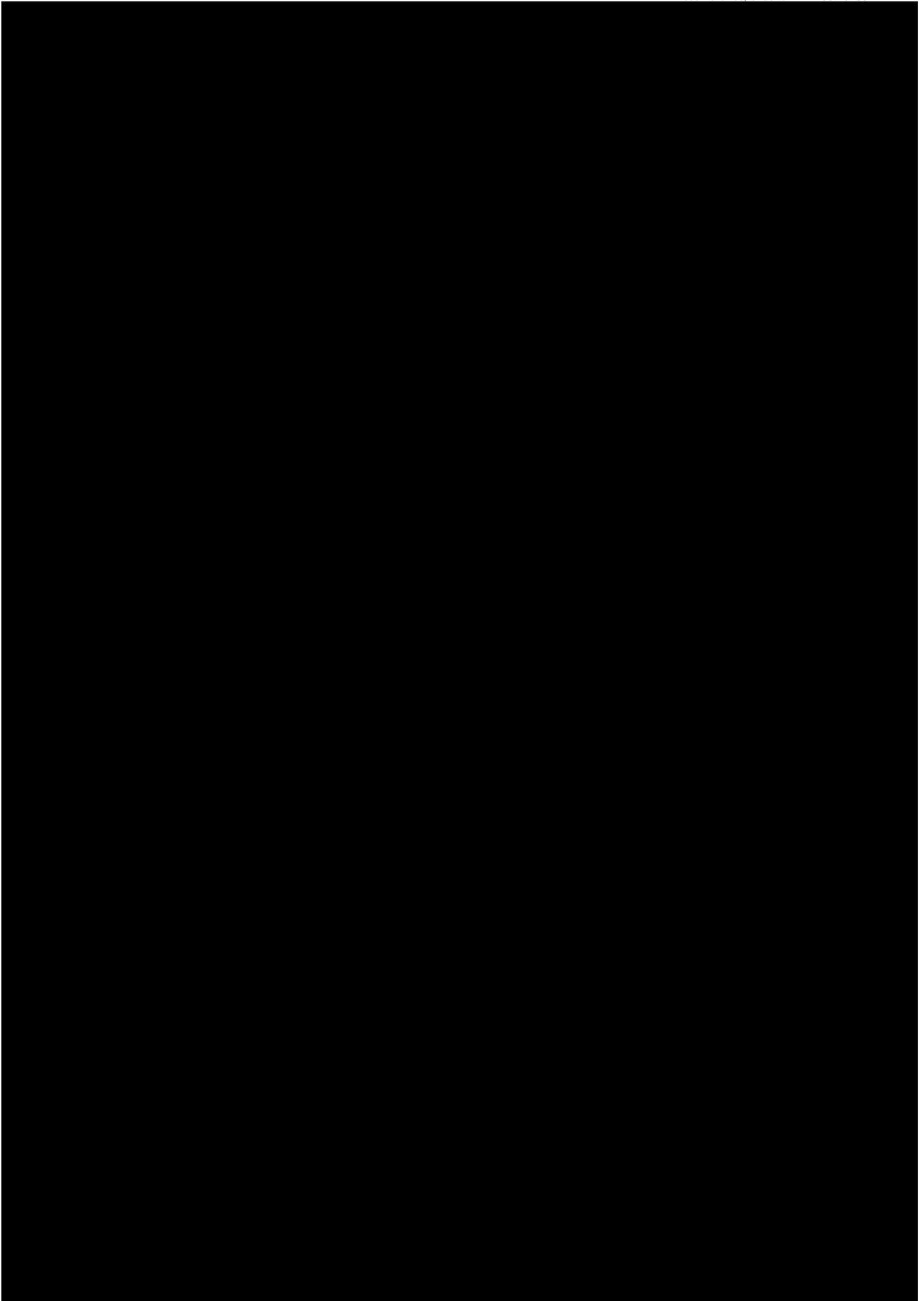
4.0 Draft Service Level Agreement

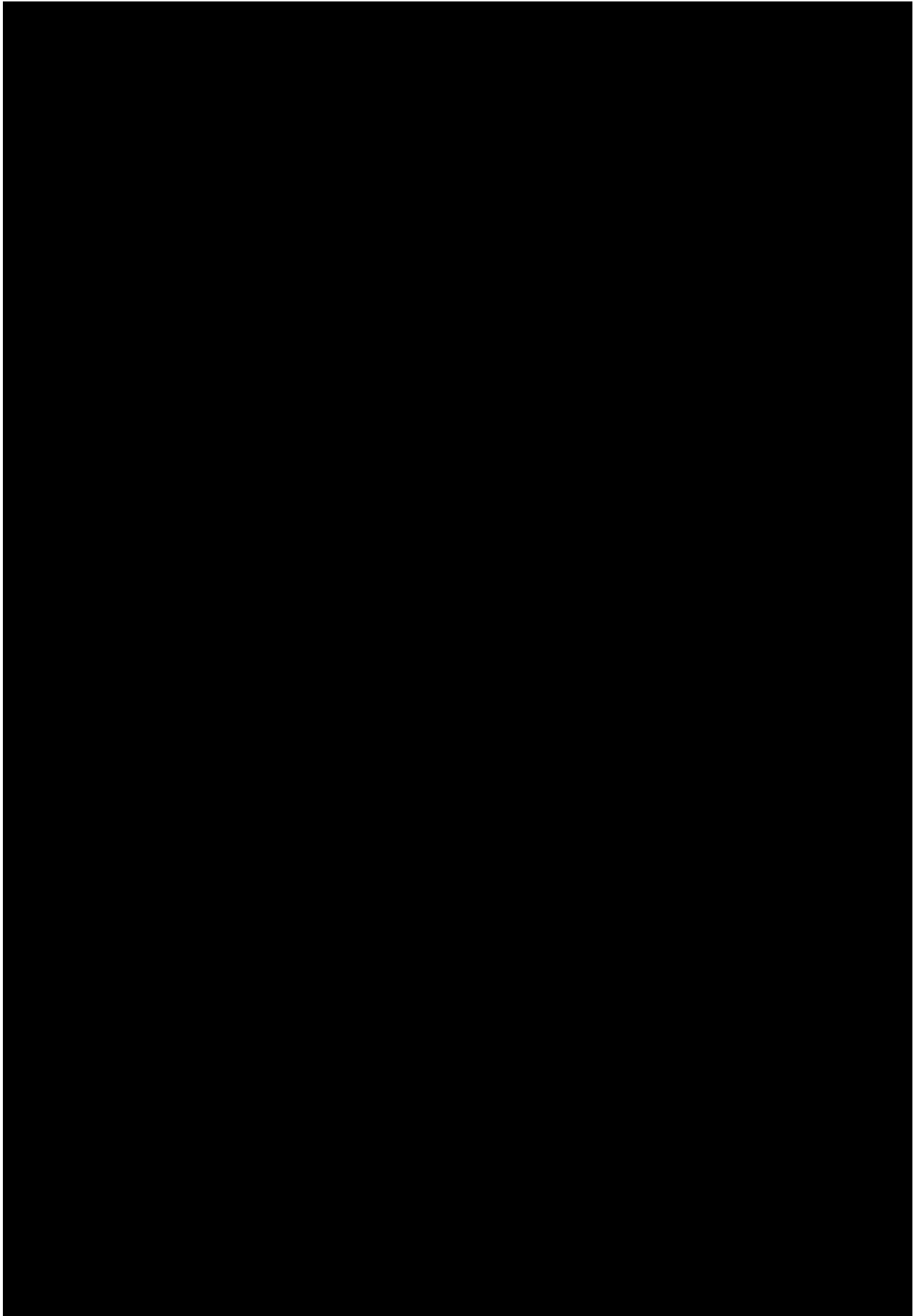
The SLA is the portion of a service contract where the level of service is formally defined between Vendor and the Agency for the delivered product(s) and/or services. The SLA will define the minimum performance and availability commitments throughout this Contract and during any renewals. The SLA will address all elements specified in RFP and will be governed by the terms and conditions in this RFP. Minimum Content:

- Commitment statements and associated performance measures pertaining to the Solution setup, testing, maintenance, uptime, response time, redundancy/failover, and Vendor support availability requirements in this RFP for the demonstration, development, testing, UAT, role-based training, maintaining production environments, and expectations for tracking and reporting;
 - Commitment statements and associated performance measures regarding the turnaround times for software application fixes, maintenance, and modifications during deployment, maintenance and support, and during and after the introduction of any modifications, enhancements, and new releases, and expectations for maintenance of technical architecture and system design documentation, role based training materials, technical and user documentation, and online help; testing; tracking; and reporting;
 - If applicable, commitment statements and performance measures ad hoc reports, queries, and/or file extracting;
 - Commitment statements and performance measures pertaining to the Help Desk support to include a description and definition of Help Desk Support, including definitions for Tier 1, Tier 2 and Tier 3 level of support; expected hours of support; expected response times; Help Desk procedures and escalation; Help Desk Roles and Responsibilities; the mechanisms for receiving service requests; and expectations for tracking and status reporting;
 - Commitment statements and performance measures to assist the State with scheduled maintenance, changes to schedule maintenance, hardware refresh, operating system (OS) updates, enterprise-level software updates, security, audits, incident response, disaster recovery (including maximum restore time and maximum failover time), and expectations for tracking and reporting;
 - Commitment statements and performance measures to assist the State with Solution performance and availability, including hours of normal operations, maintenance windows, online backup time ranges, batch time ranges, maximum planned downtime per week, maximum unplanned downtime during normal business hours per month, hours of Solution availability, state of emergency hours of operation, average retention period for online data, and offline backup time range, and expectations for tracking and reporting;
 - Definitions of service requests and problem categories;
 - Escalation procedures for each problem category;
 - A description of the procedures, monitoring tools, and reports used to ensure compliance with these commitments. The report will use a format agreed upon by the State;
 - Penalties for noncompliance with the terms of the SLA
-









13. Solution Operations Key Areas

A. Solution Setup

Commitment statements and associated performance measures pertaining to the Solution setup, testing, maintenance, uptime, response time, redundancy/failover, and Vendor support availability requirements in this RFP for the demonstration, development, testing, UAT, role-based training, maintaining production environments, and expectations for tracking and reporting;

Please refer to Attachment 1 and Attachment 2 in this document for commitment statements and associated performance measures pertaining to Solution Setup.

B. Solution Application Maintenance

Commitment statements and associated performance measures regarding the turnaround times for software application fixes, maintenance, and modifications during deployment, maintenance and support, and during and after the introduction of any modifications, enhancements, and new releases, and expectations for maintenance of technical architecture and system design documentation, role based training materials, technical and user documentation, and

Please refer to Attachment 1 and Attachment 2 in this document for commitment statements and associated performance measures pertaining to Solution Application Maintenance.

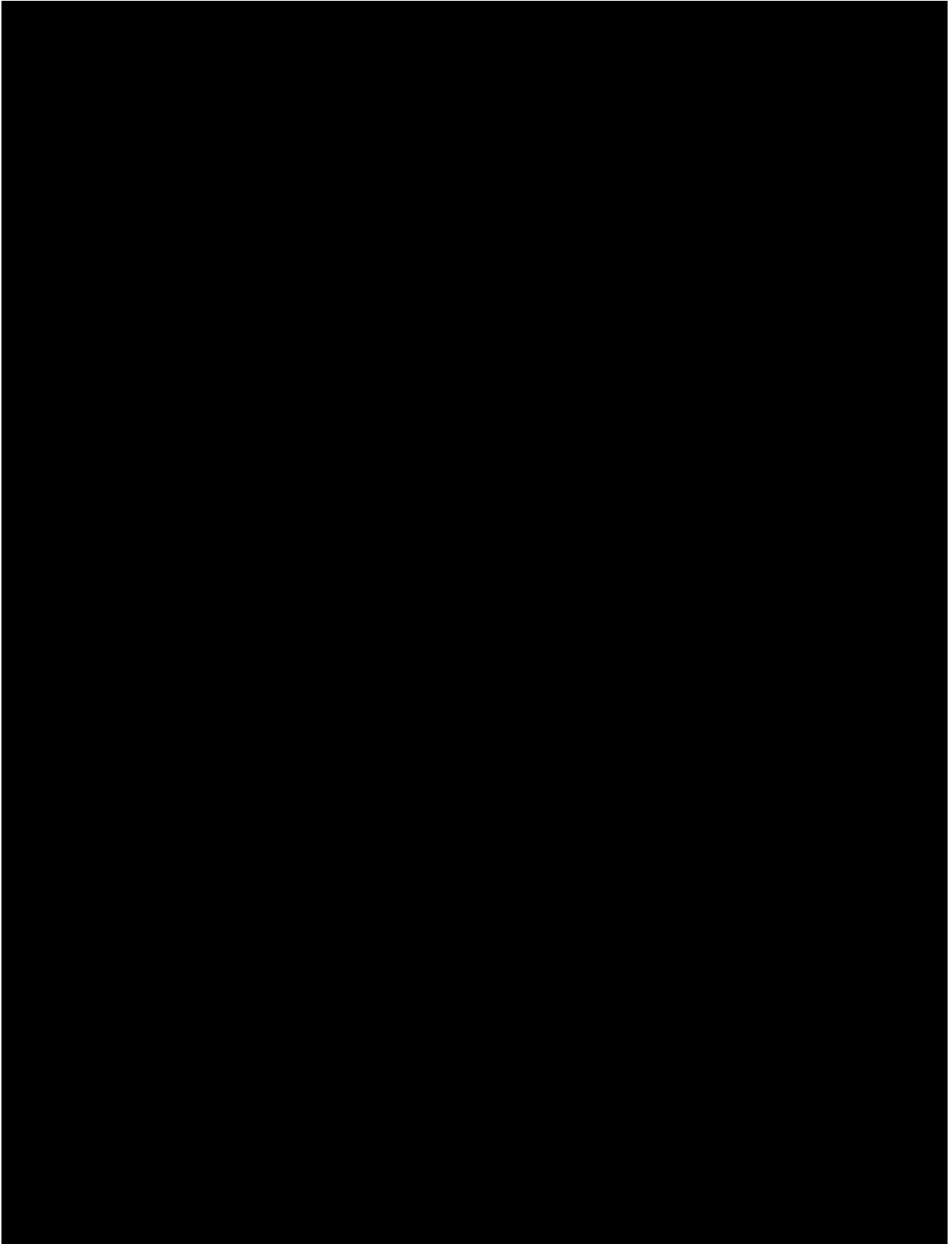
C. Reporting

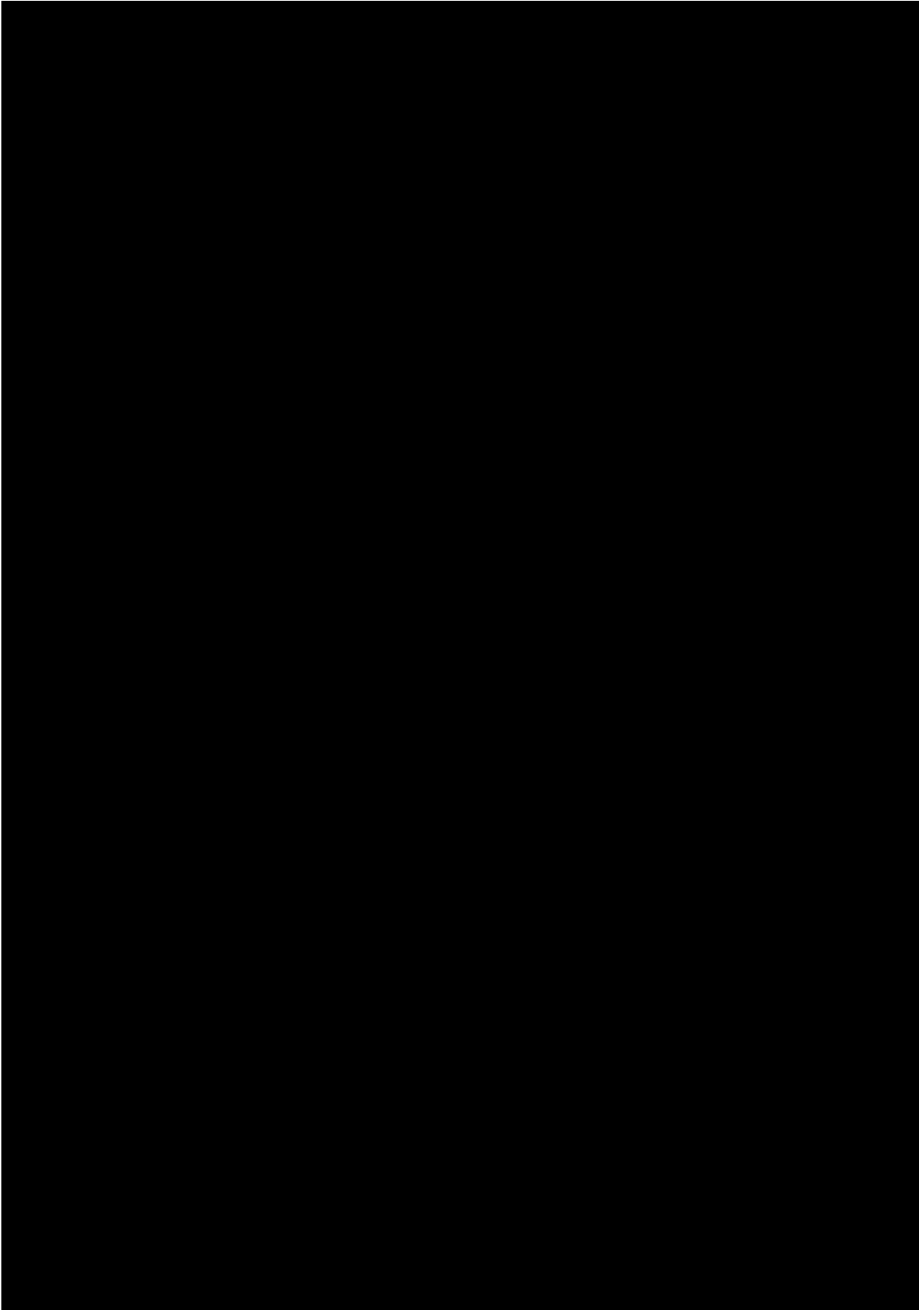
If applicable, commitment statements and performance measures for ad hoc reports, queries, and/or file extracting;

Ad hoc reports and query requests will be treated as Category 5 Service Requests. Performance Measures for Service Requests are defined in Attachment 1 and Attachment 2 of this document.

D. Help Desk

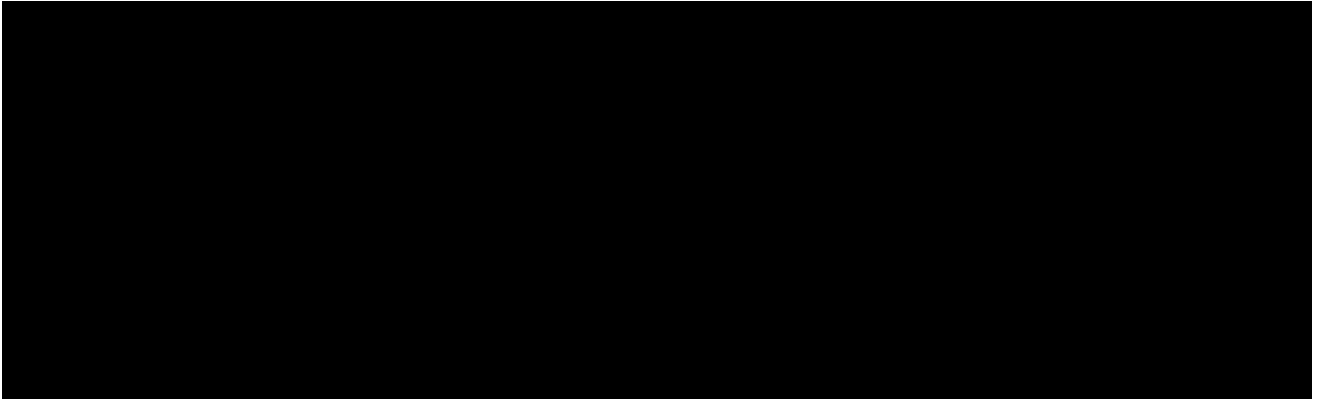
Commitment statements and performance measures pertaining to the Help Desk support to include a description and definition of Help Desk Support, including definitions for Tier 1, Tier 2 and Tier 3 level of support; expected hours of support; expected response times; Help Desk procedures and escalation; Help Desk Roles and Responsibilities; the mechanisms for receiving service requests; and expectations for tracking and status reporting;





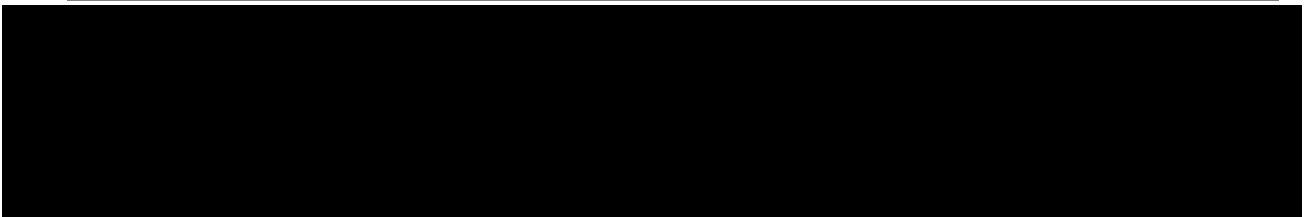
E. Solution Infrastructure Maintenance

Commitment statements and performance measures to assist the State with scheduled maintenance, changes to schedule maintenance, hardware refresh, operating system (OS) updates, enterprise-level software updates, security, audits, incident response, disaster recovery (including maximum restore time and maximum failover time), and expectations for tracking and reporting;



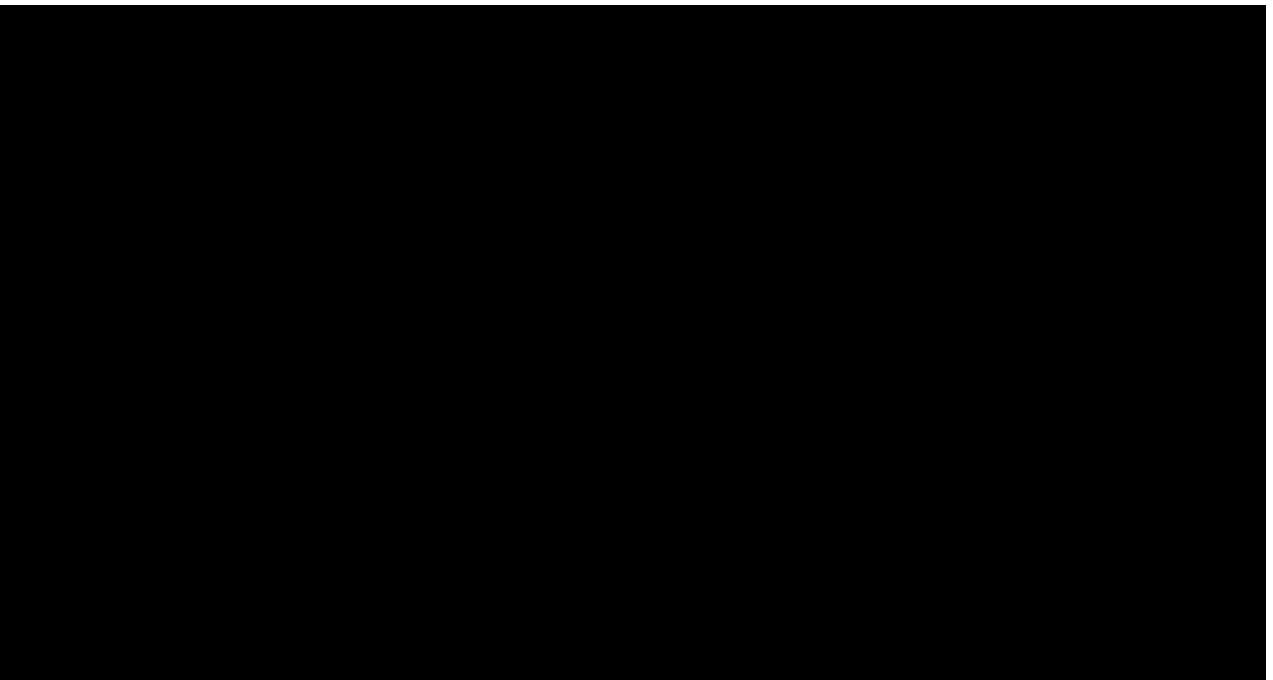
F. Solution Performance and Availability

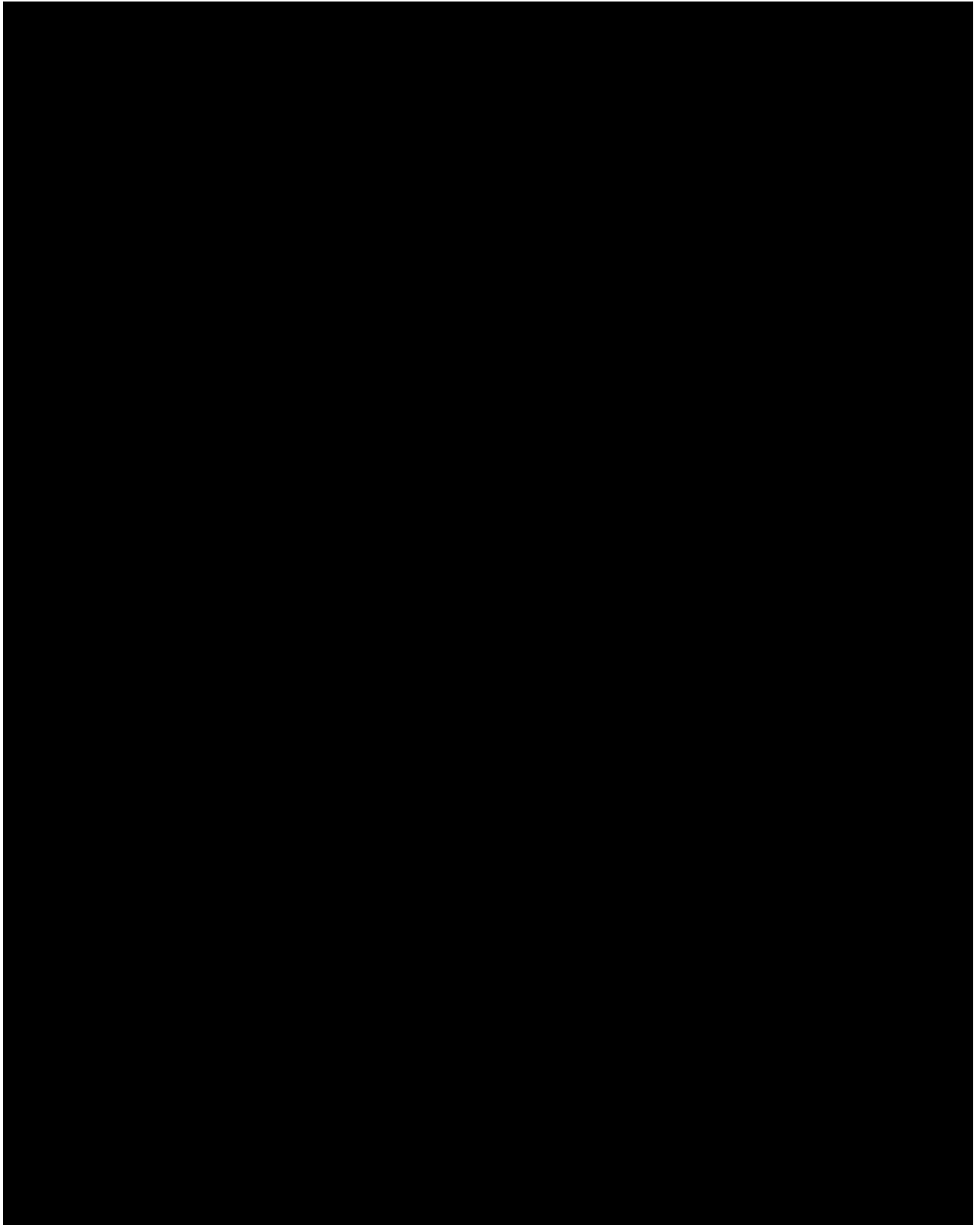
Commitment statements and performance measures to assist the State with Solution performance and availability, including hours of normal operations, maintenance windows, online backup time ranges, batch time ranges, maximum planned downtime per week, maximum unplanned downtime during normal business hours per month, hours of Solution availability, state of emergency hours of operation, average retention period for online data, and offline backup time range, and expectations for tracking and reporting;

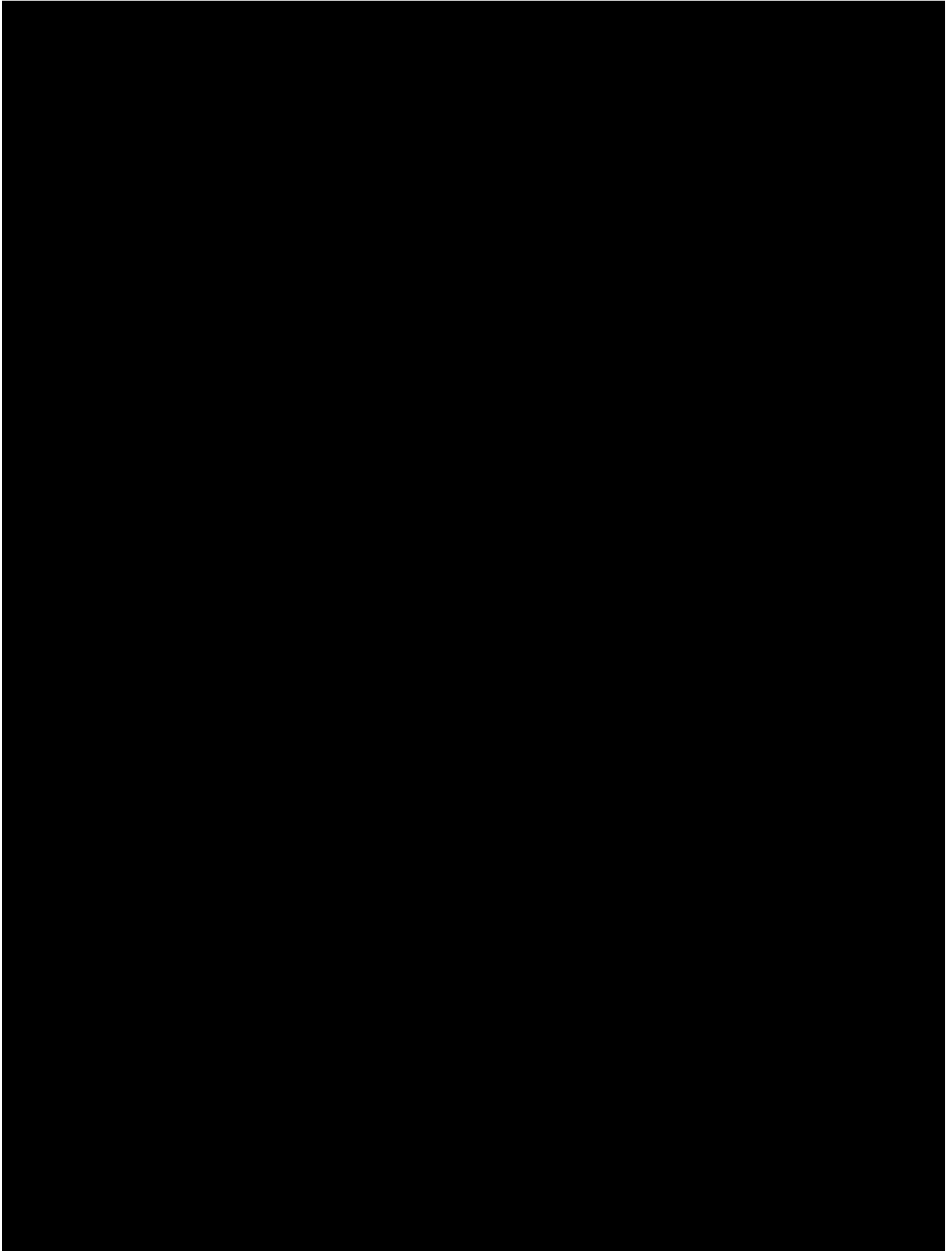


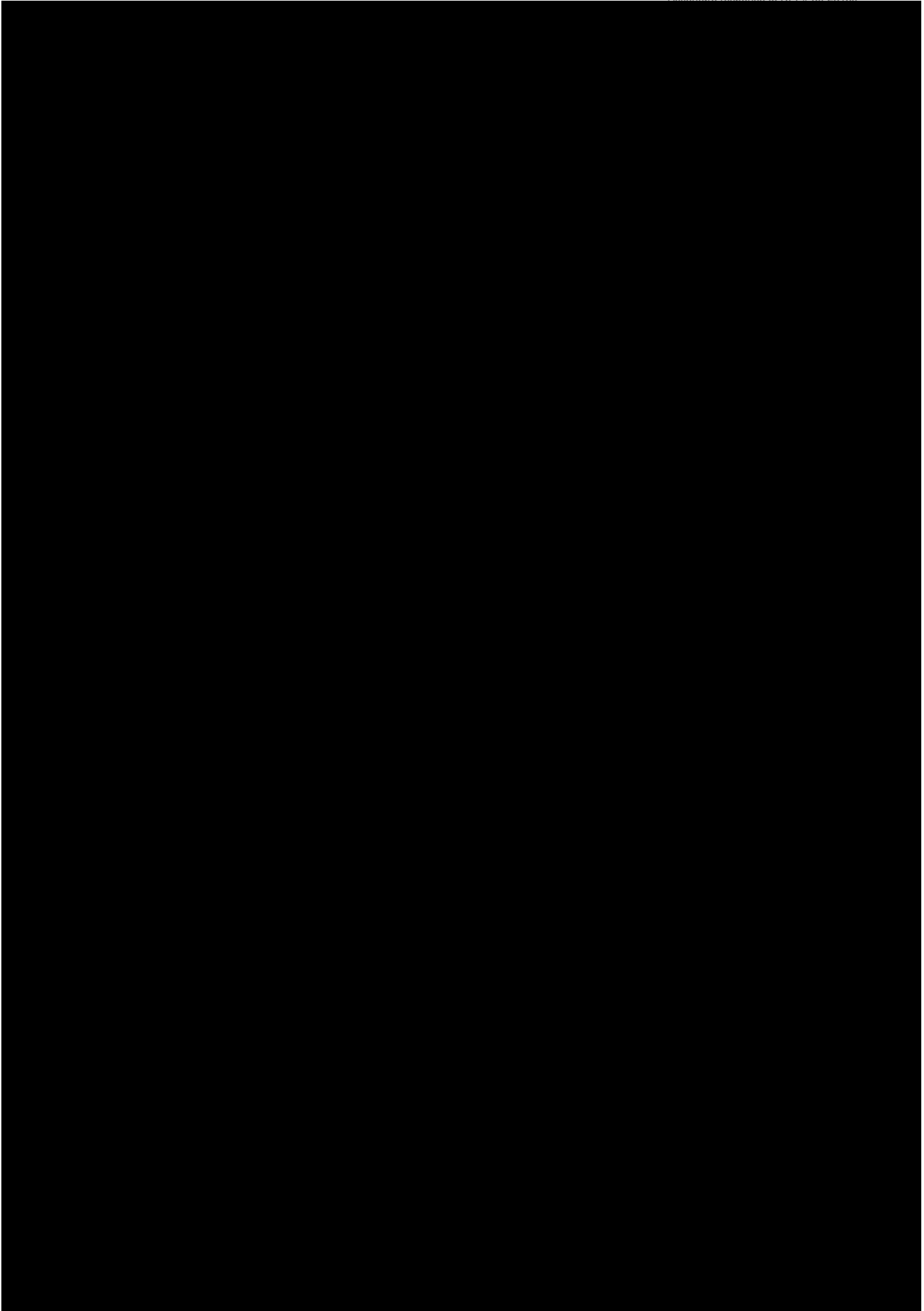
G. Service Request / Problem Category Definitions

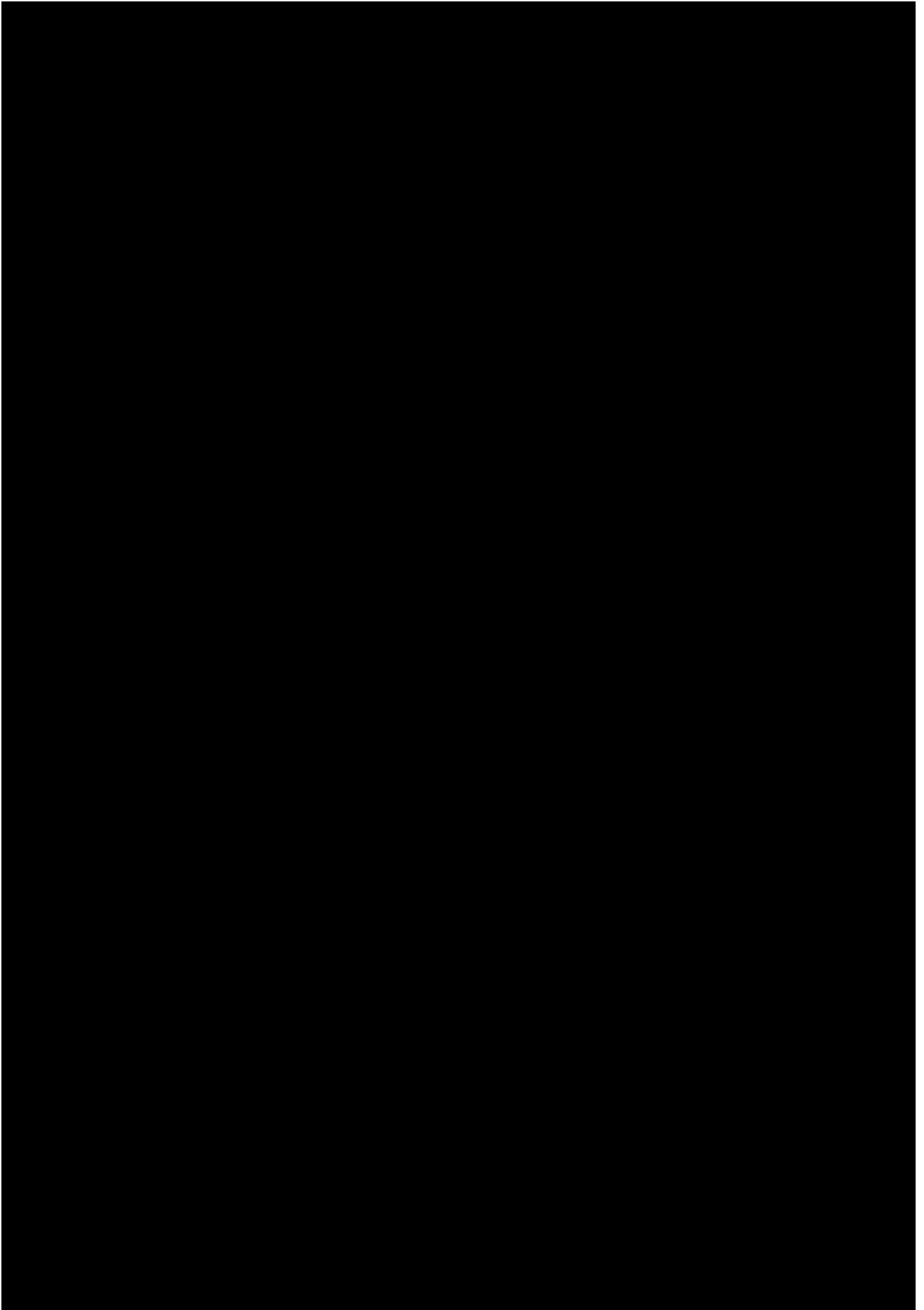
Definitions of service requests and problem categories;

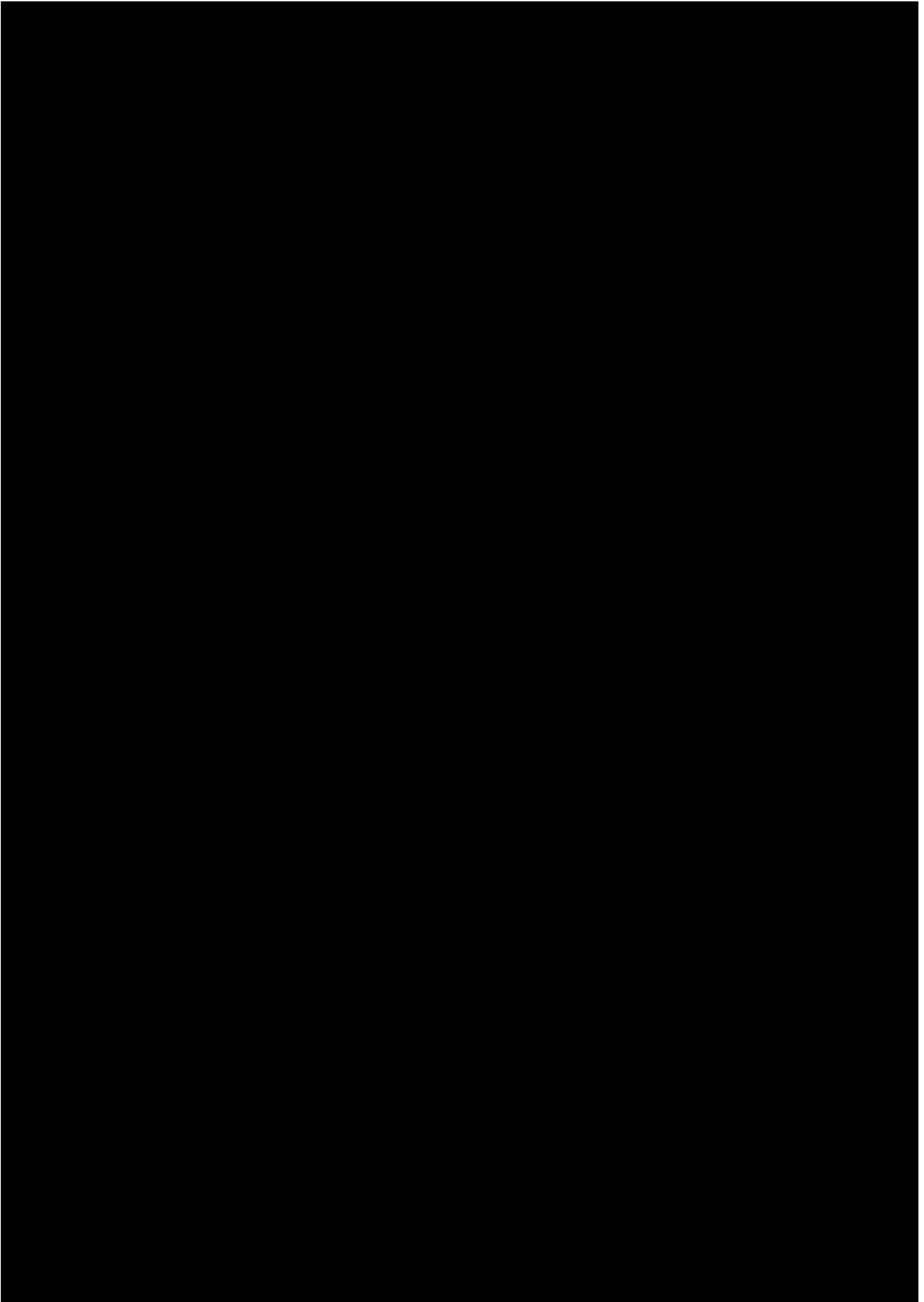


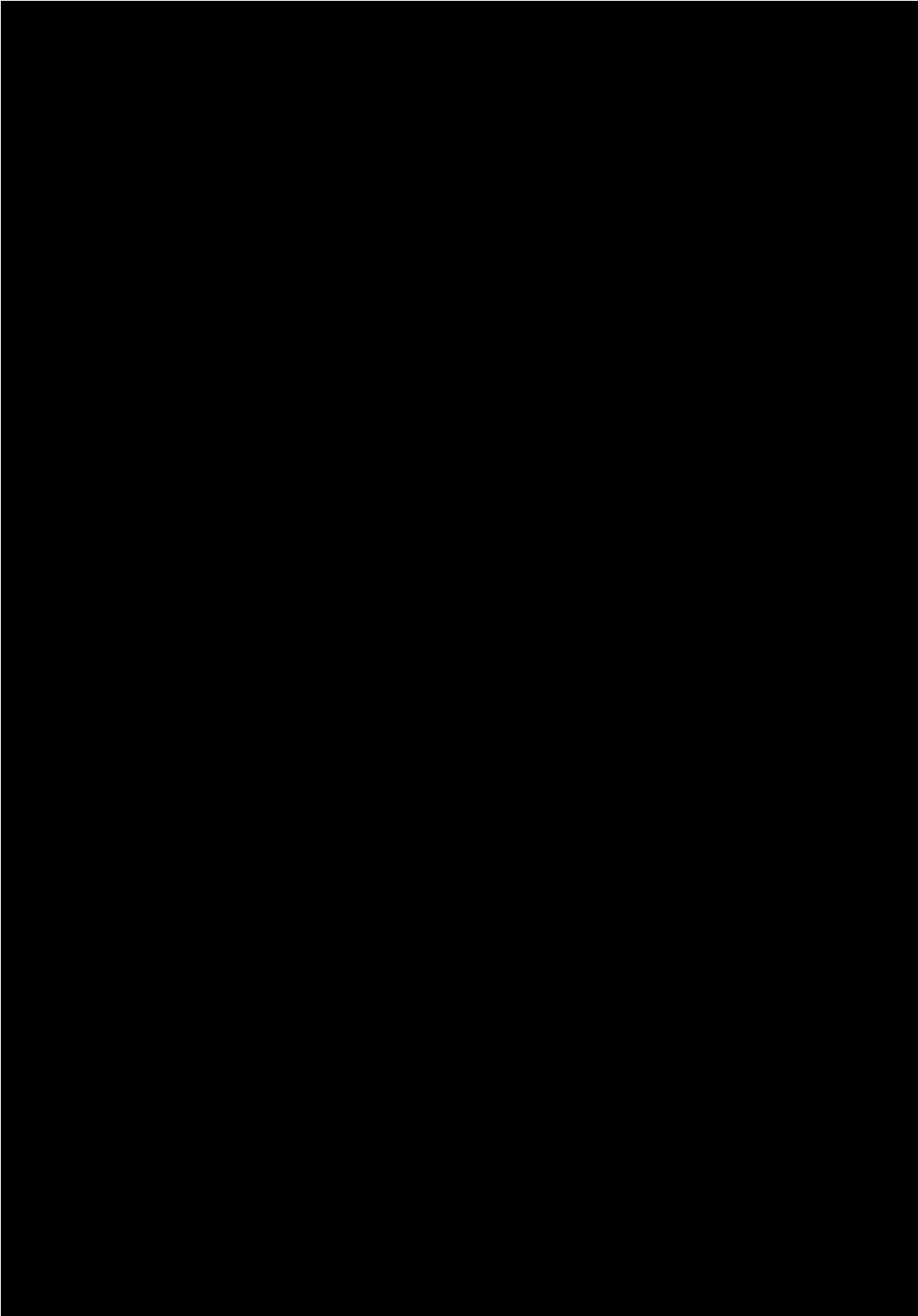


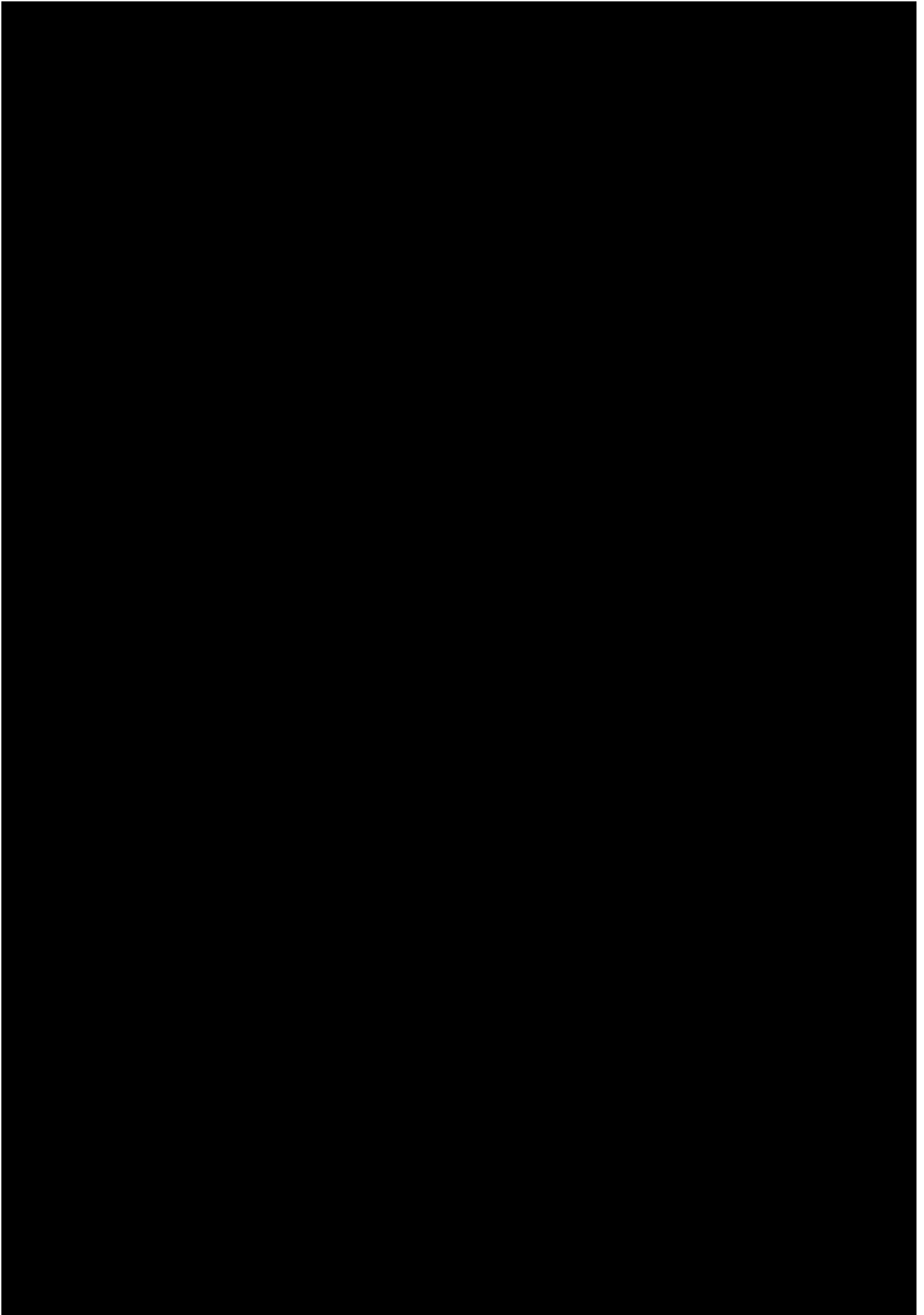


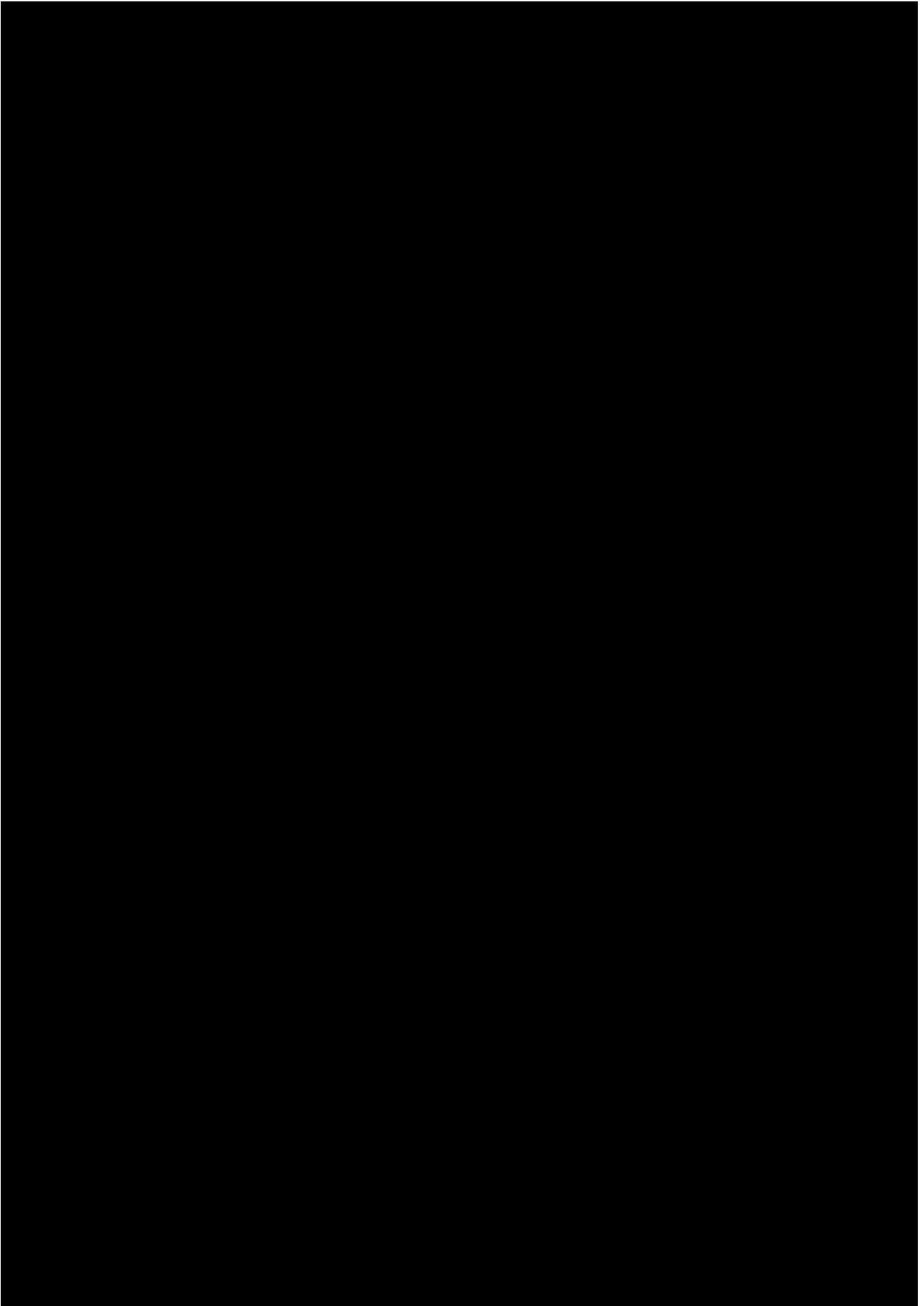


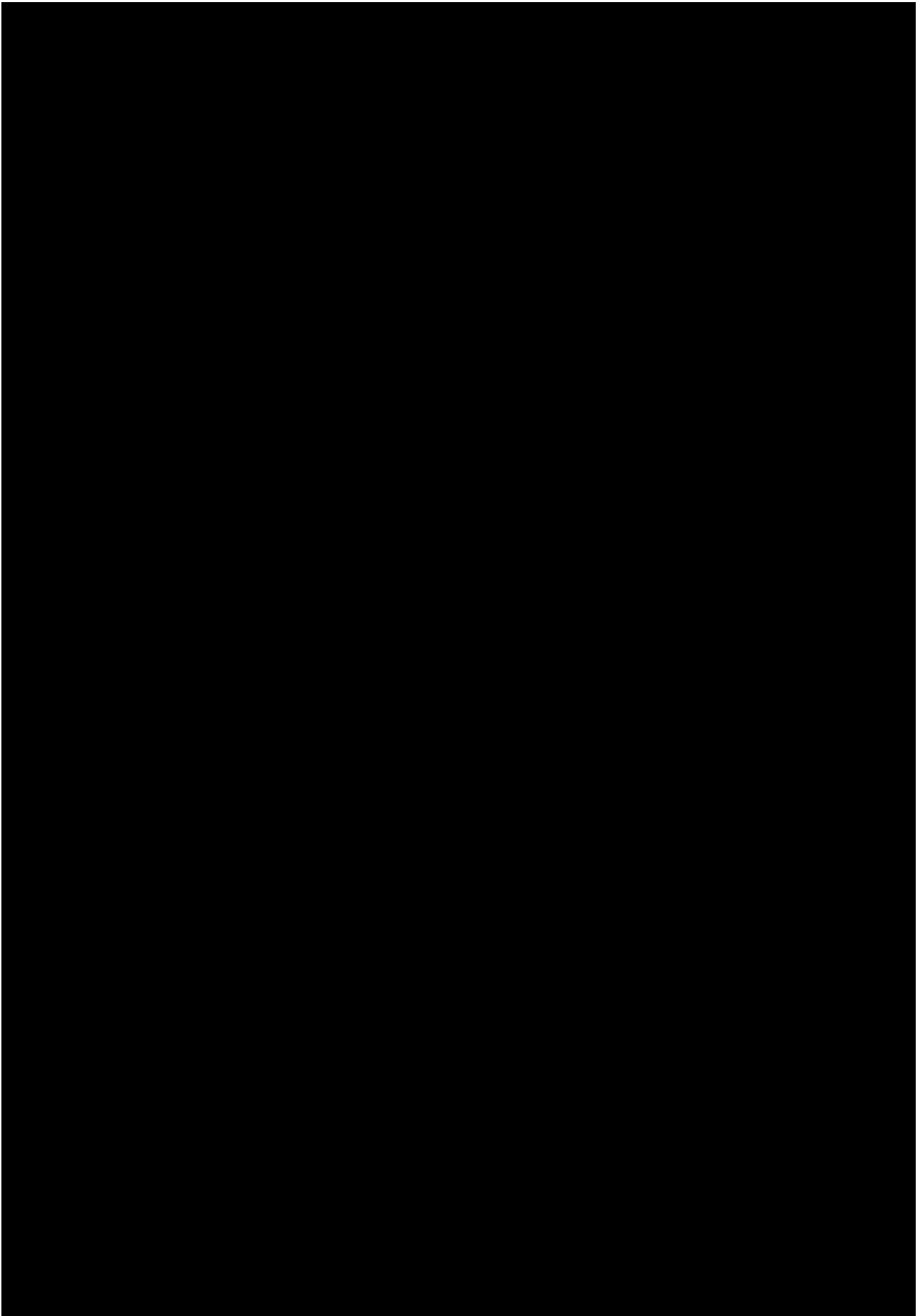


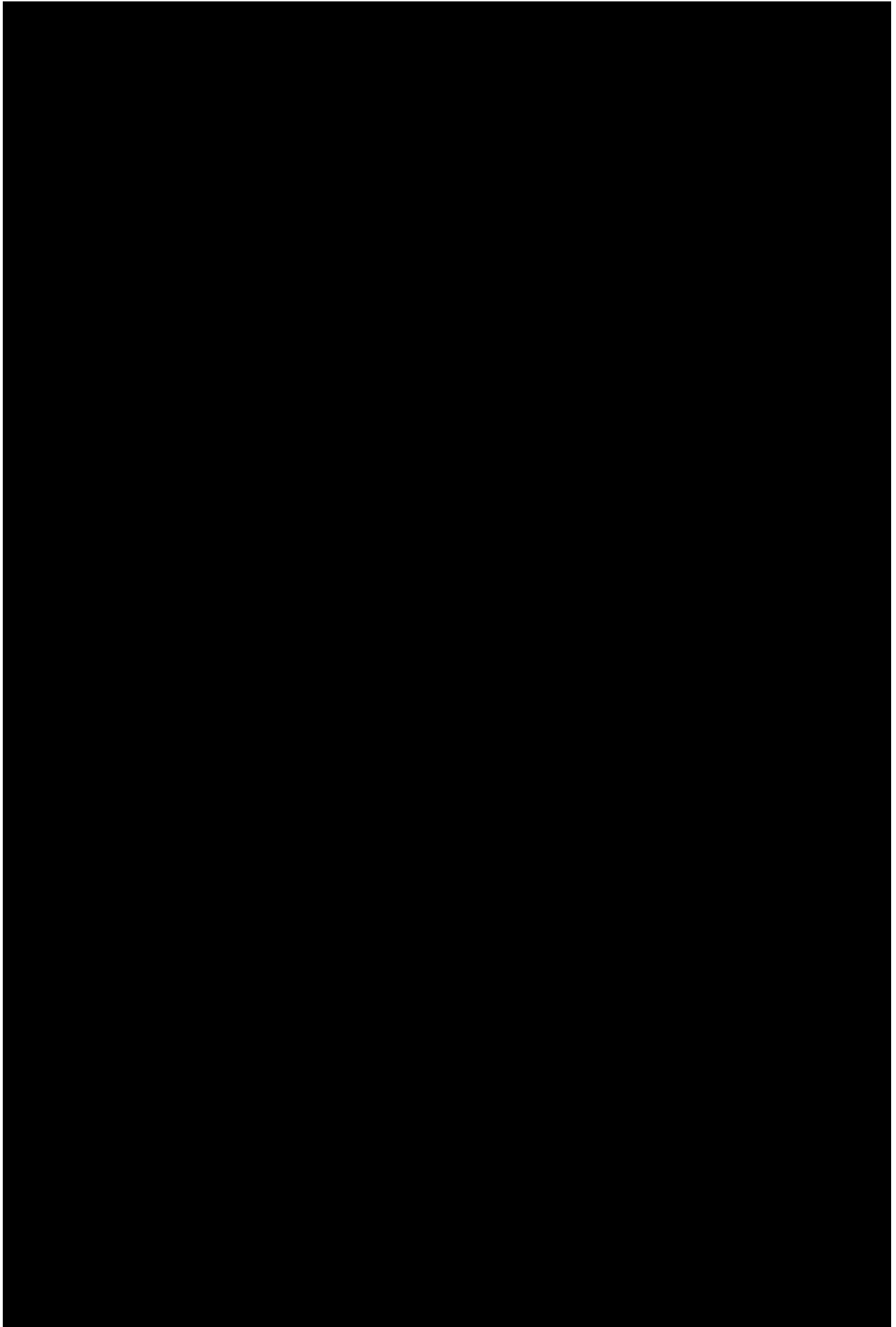


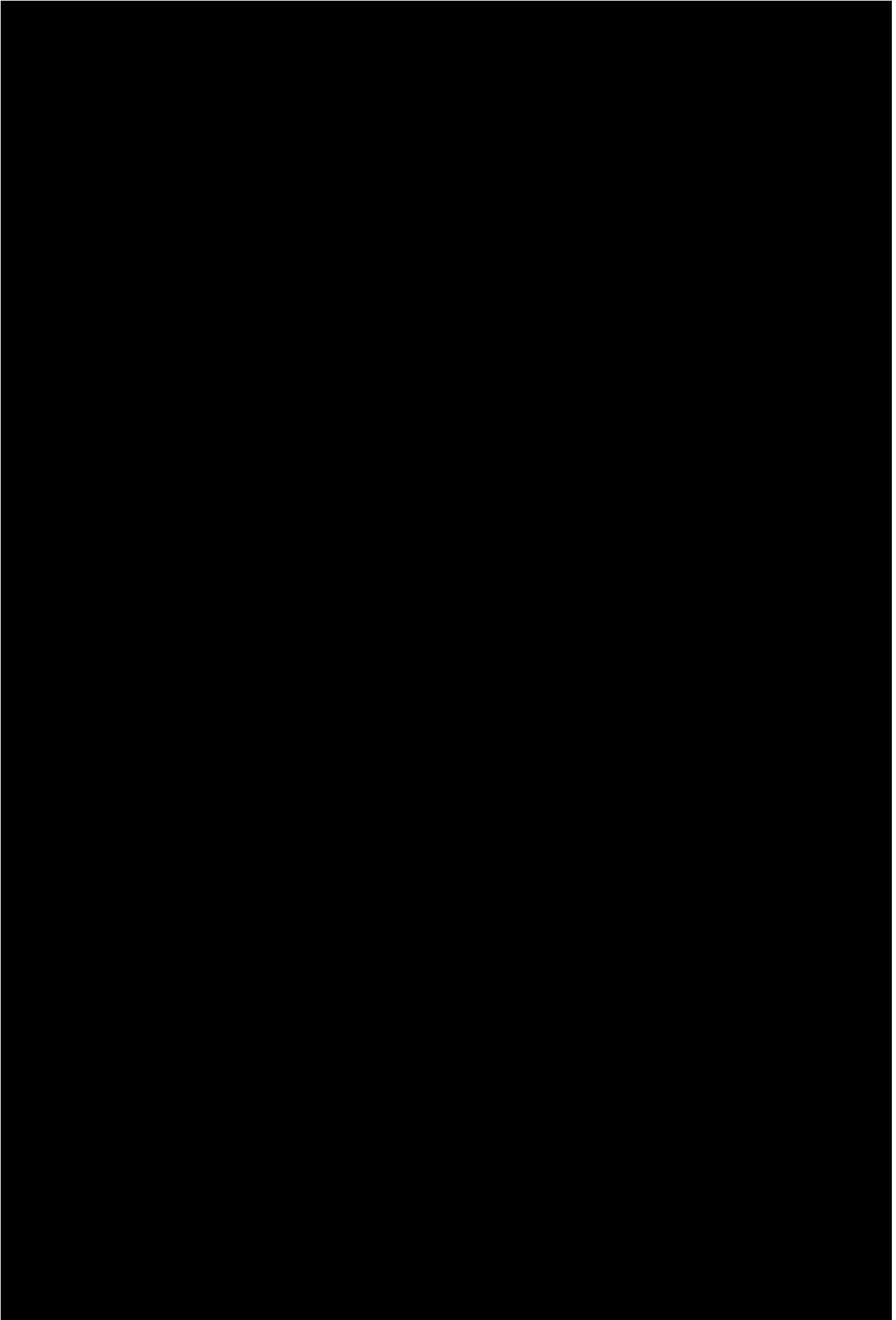


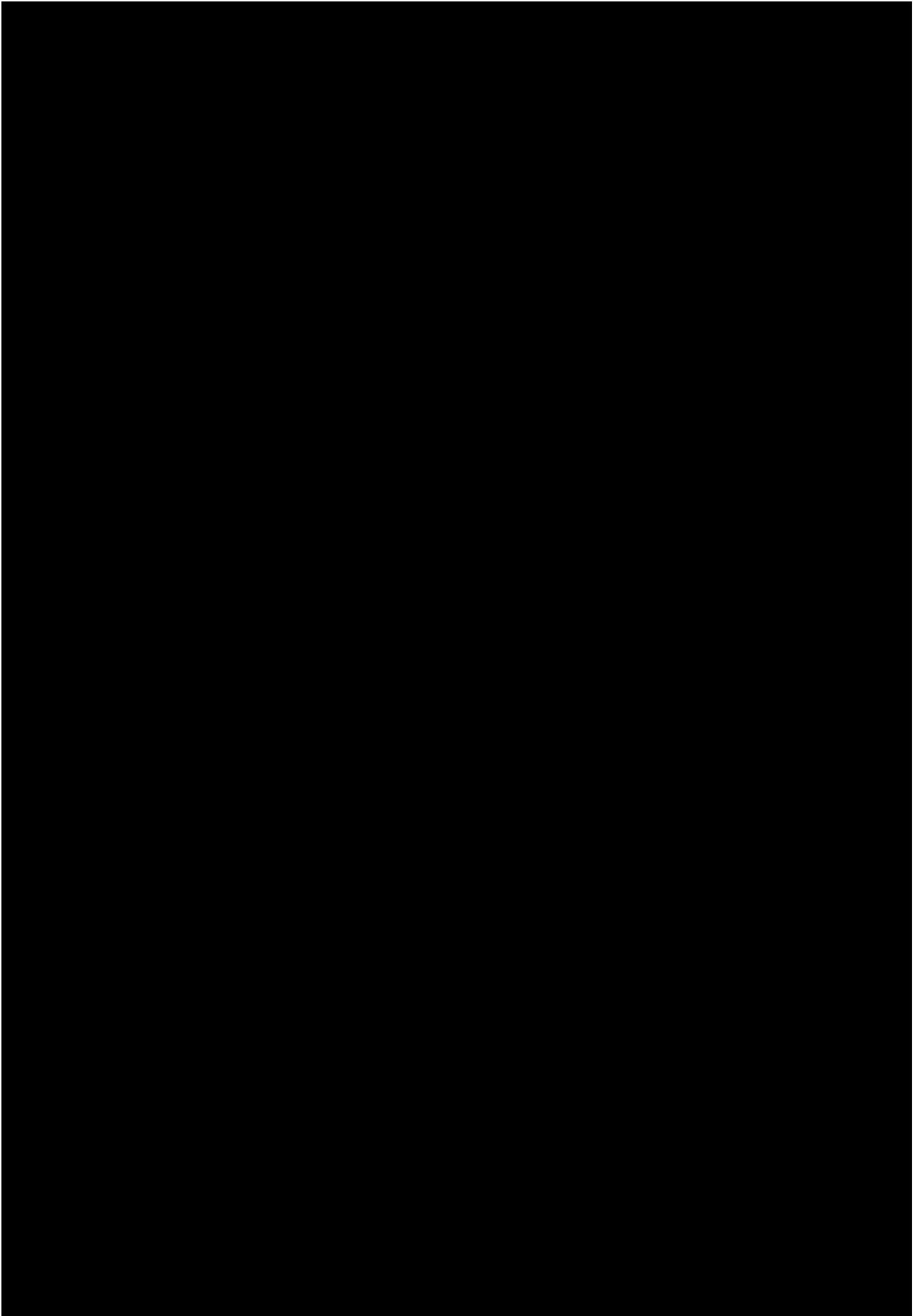


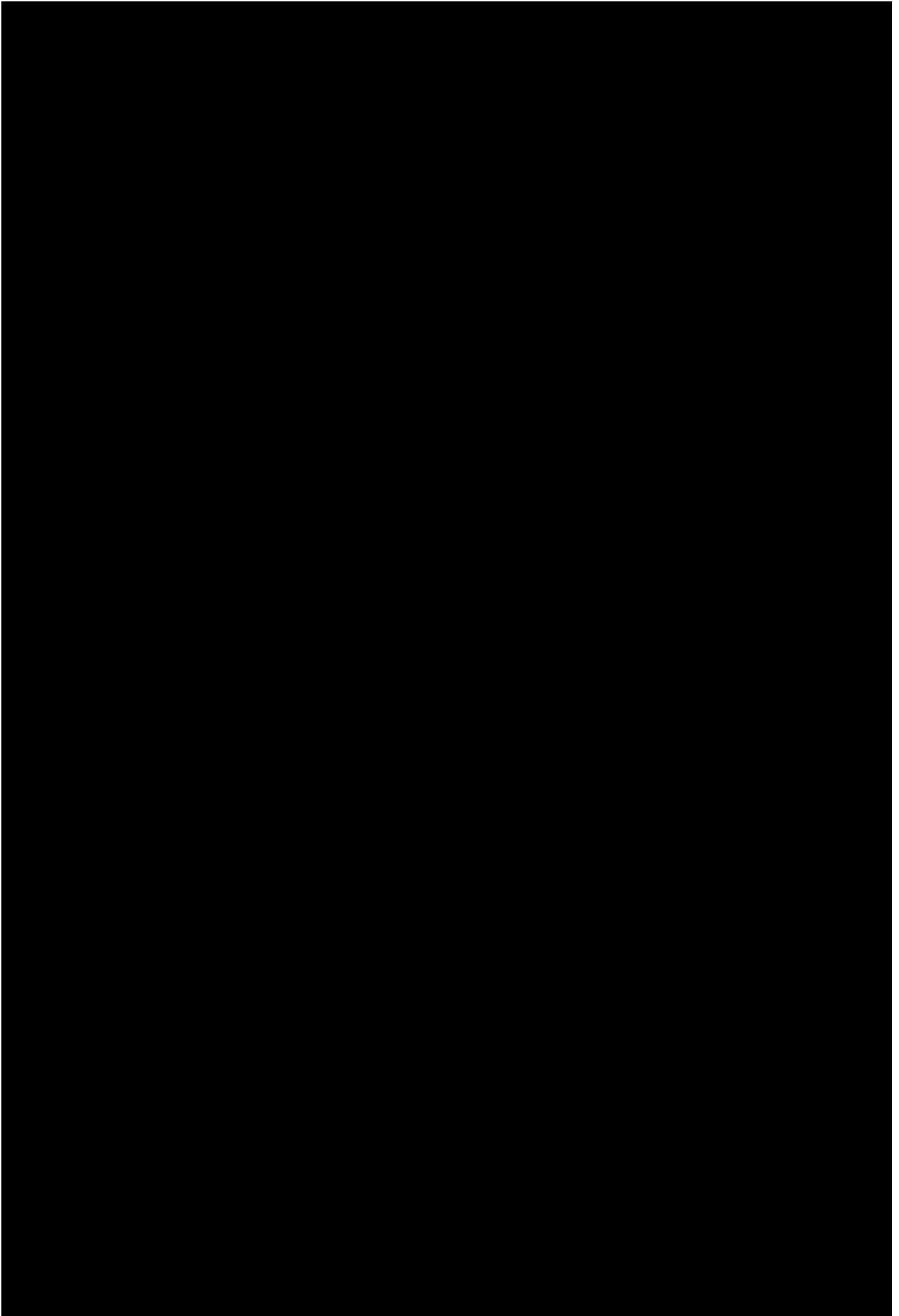


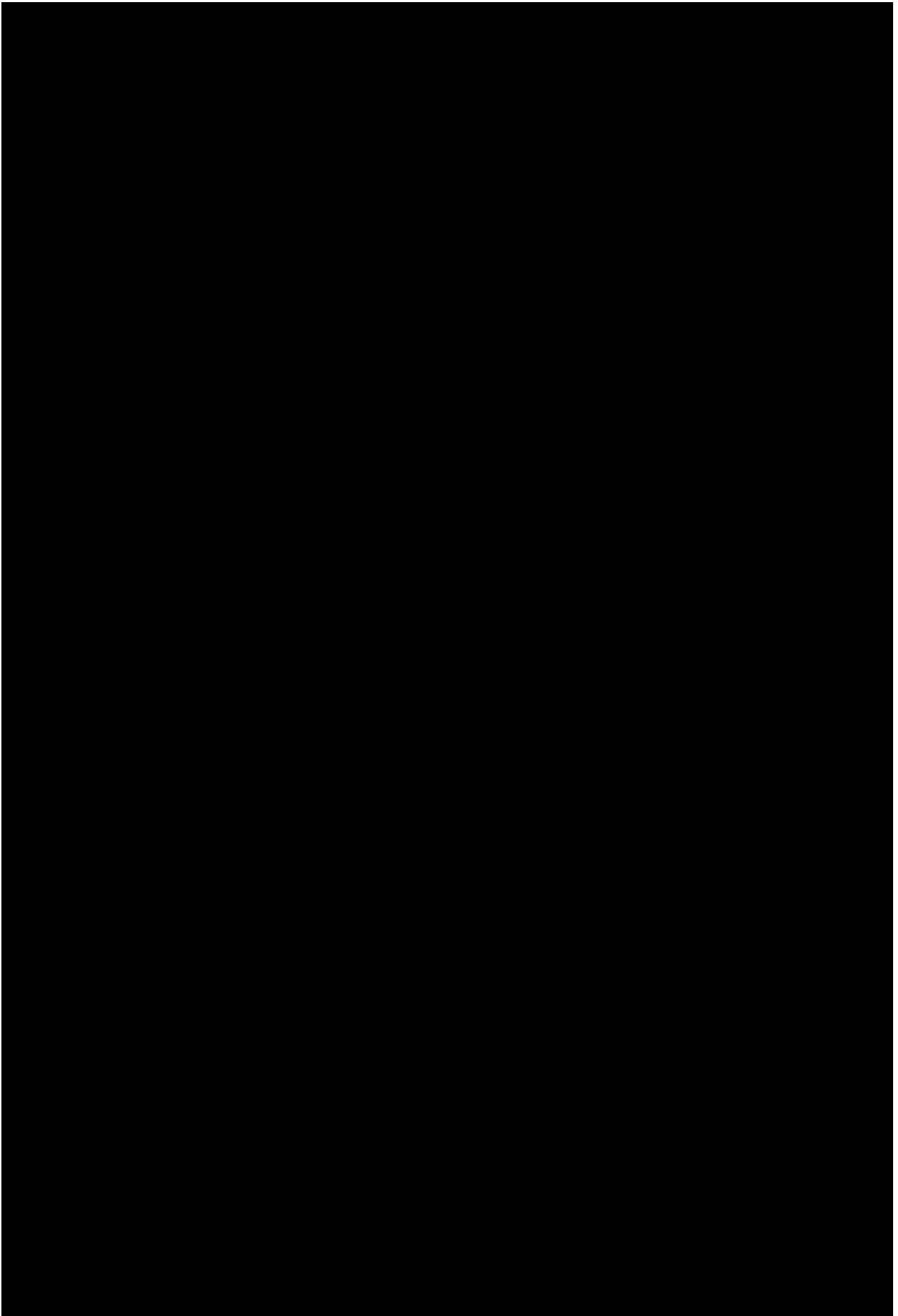


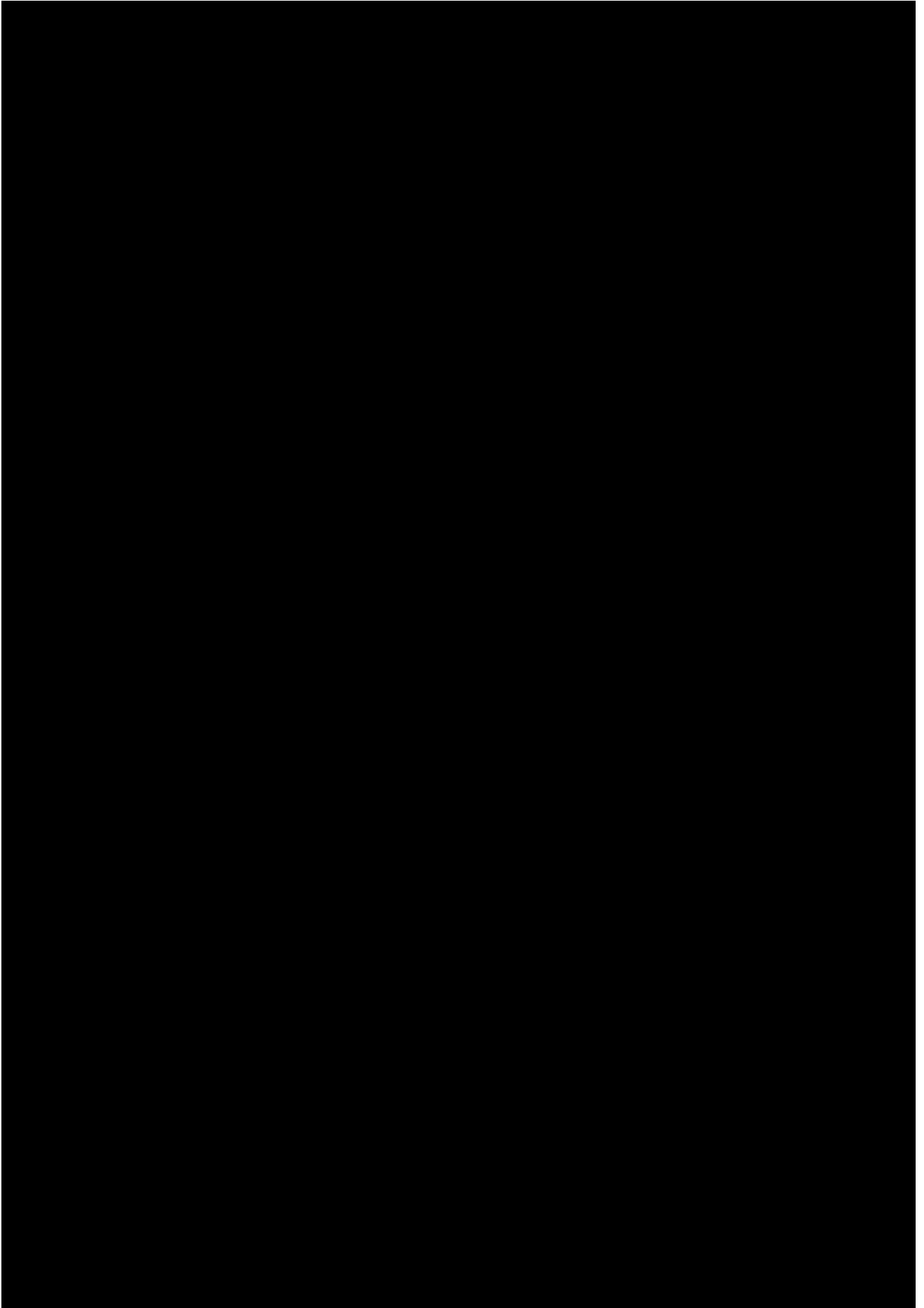


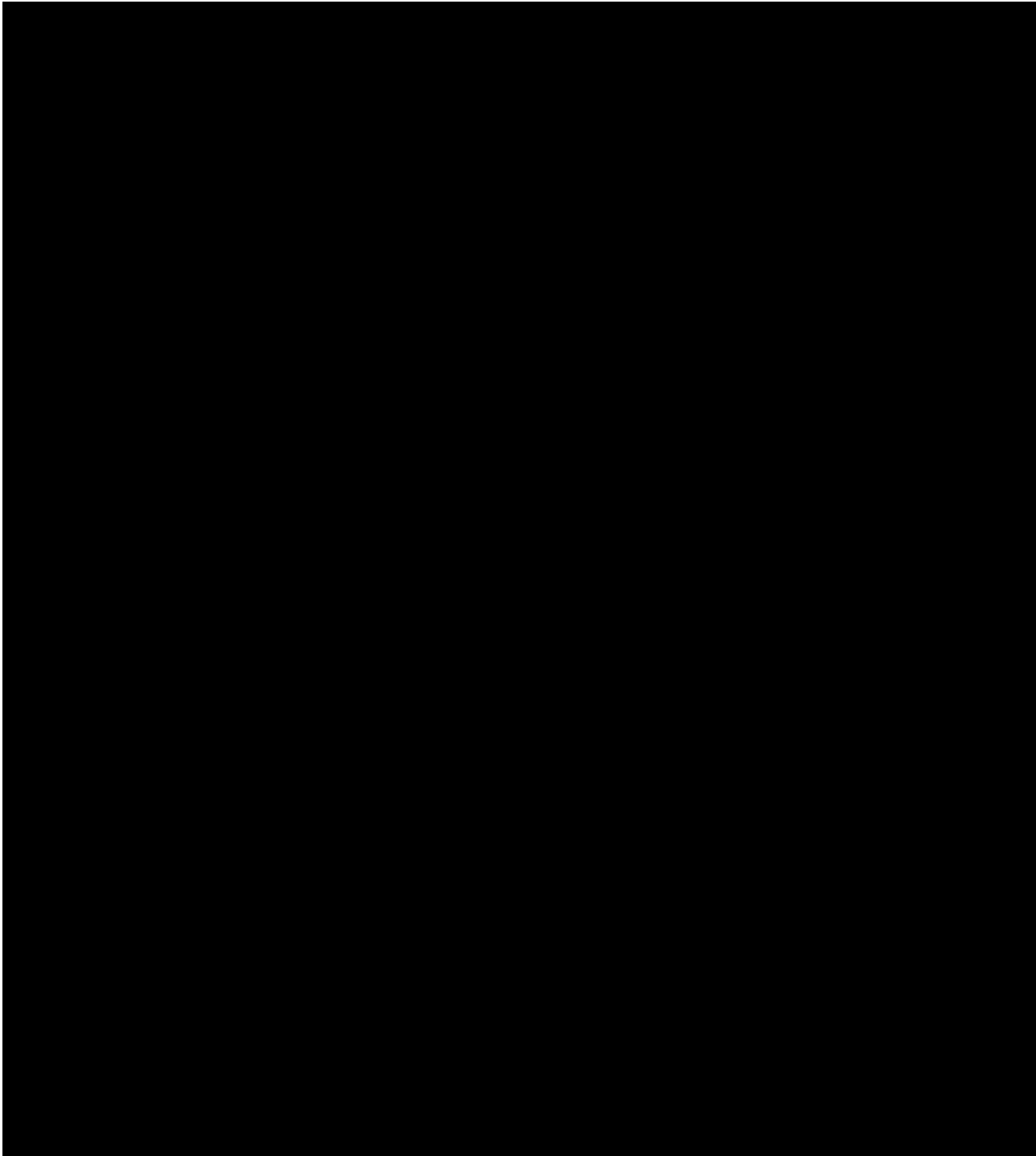








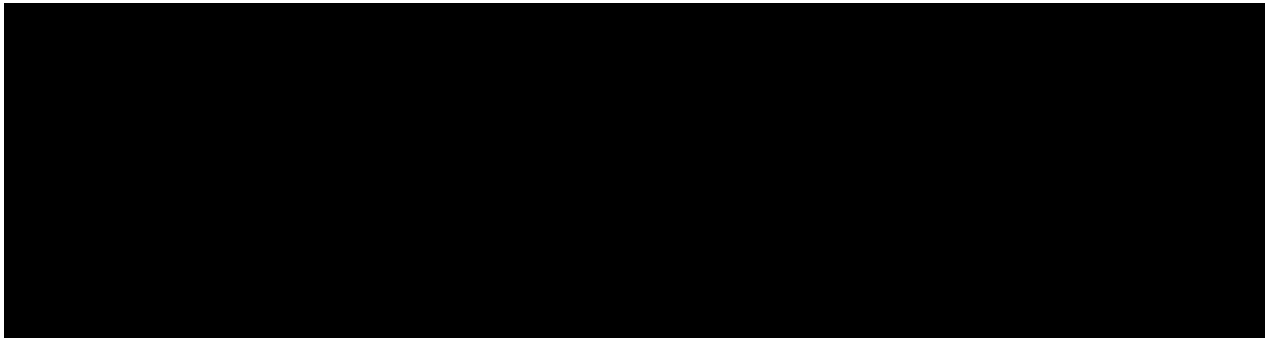




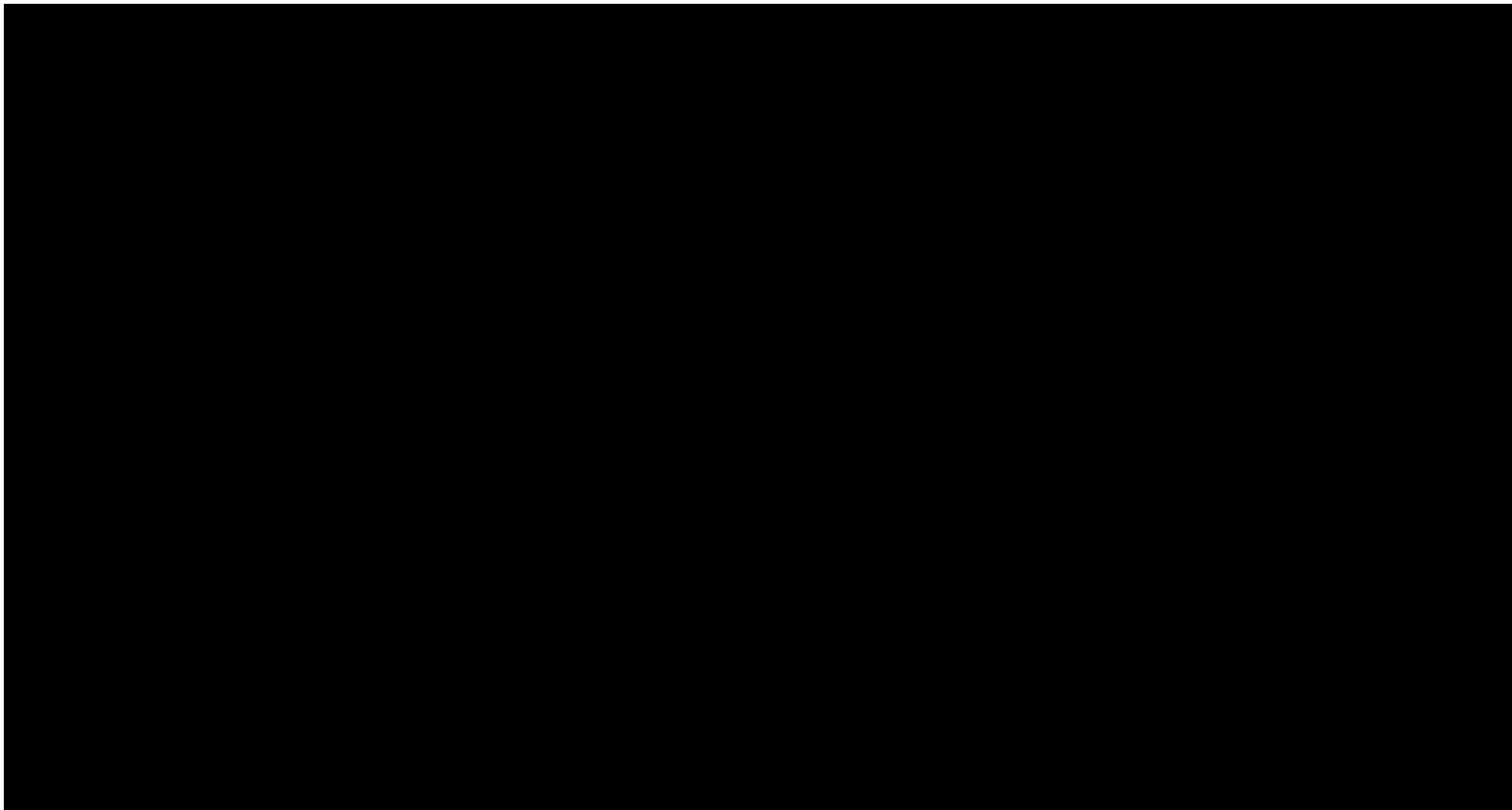
5.0 Draft Operations and Maintenance Phase Staffing Plan

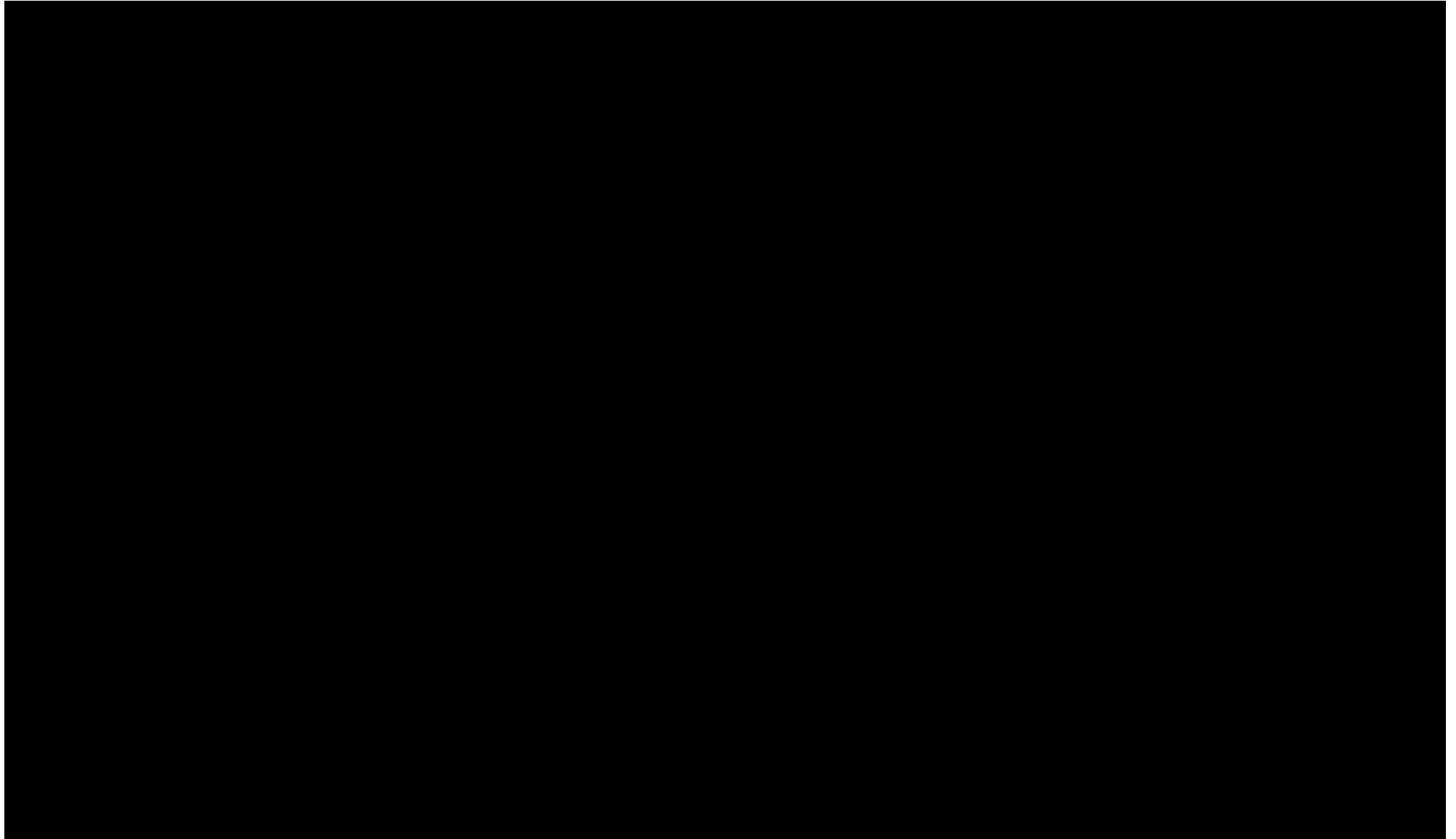
The Vendor O&M Staffing Plan contains the amounts of Vendor labor resources needed to accomplish tasks during the O&M Contract Phase of the Contract. Minimum Content:

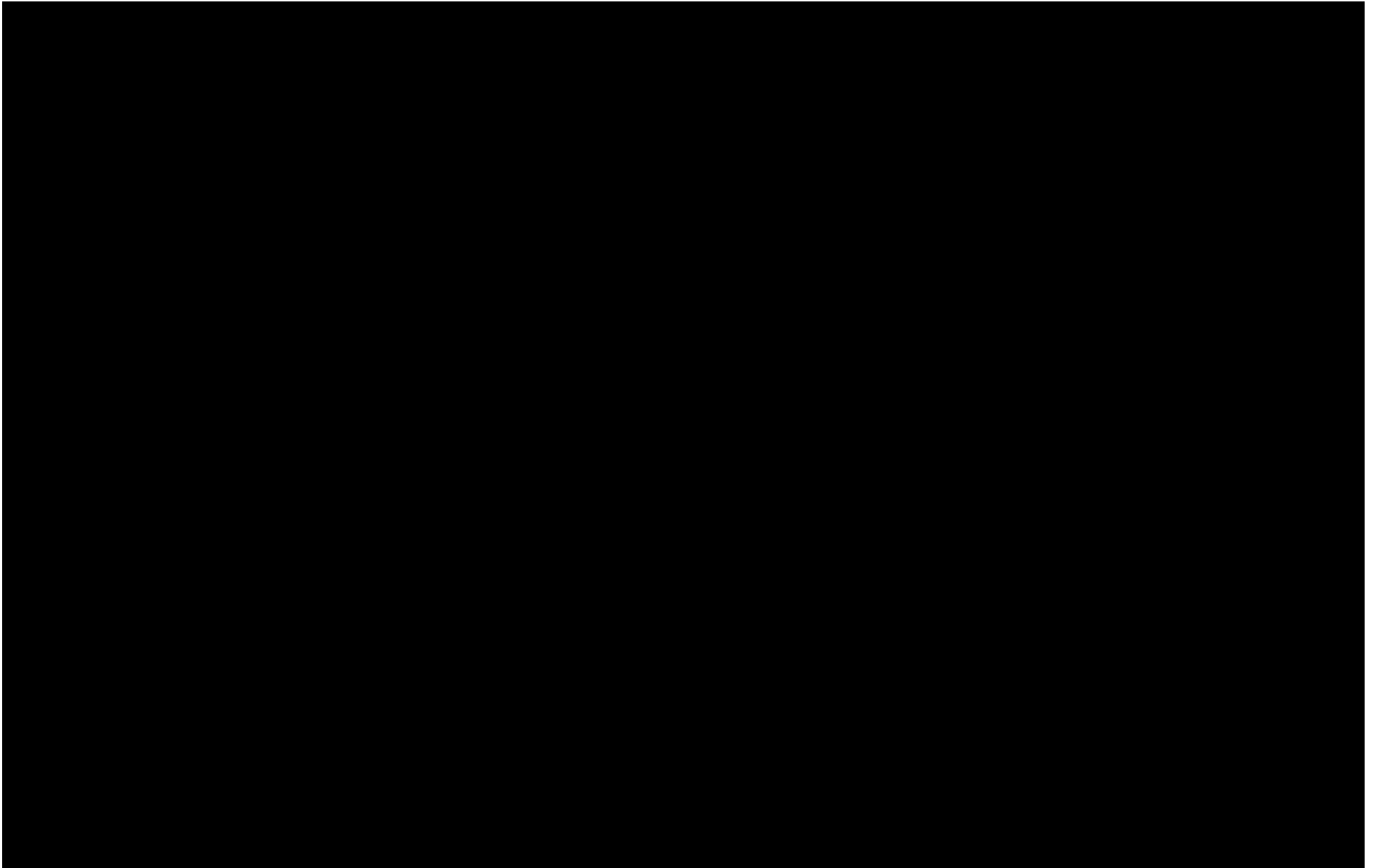
- Identify each person who will be assigned during the O&M Contract Phase as required to ensure SLA requirements can be met, including any subcontractors.
 - Roles and responsibilities for Vendor and subcontractors.
 - Vendor organizational information, including an organizational chart (if different from organization information submitted with the Vendor Project Staffing Plan);
 - The number of dedicated FTEs and the percentage of each resource's time during the O&M Contract Phase.
 - The estimated hours per resource.
 - How long each resource will work during the O&M Contract Phase.
 - A matrix of required skills/roles for each resource.
 - Vendor's specifications for State resources and the duration and type of each State resource requirement.
 - Other Vendor resources available to the Agency during O&M.
-

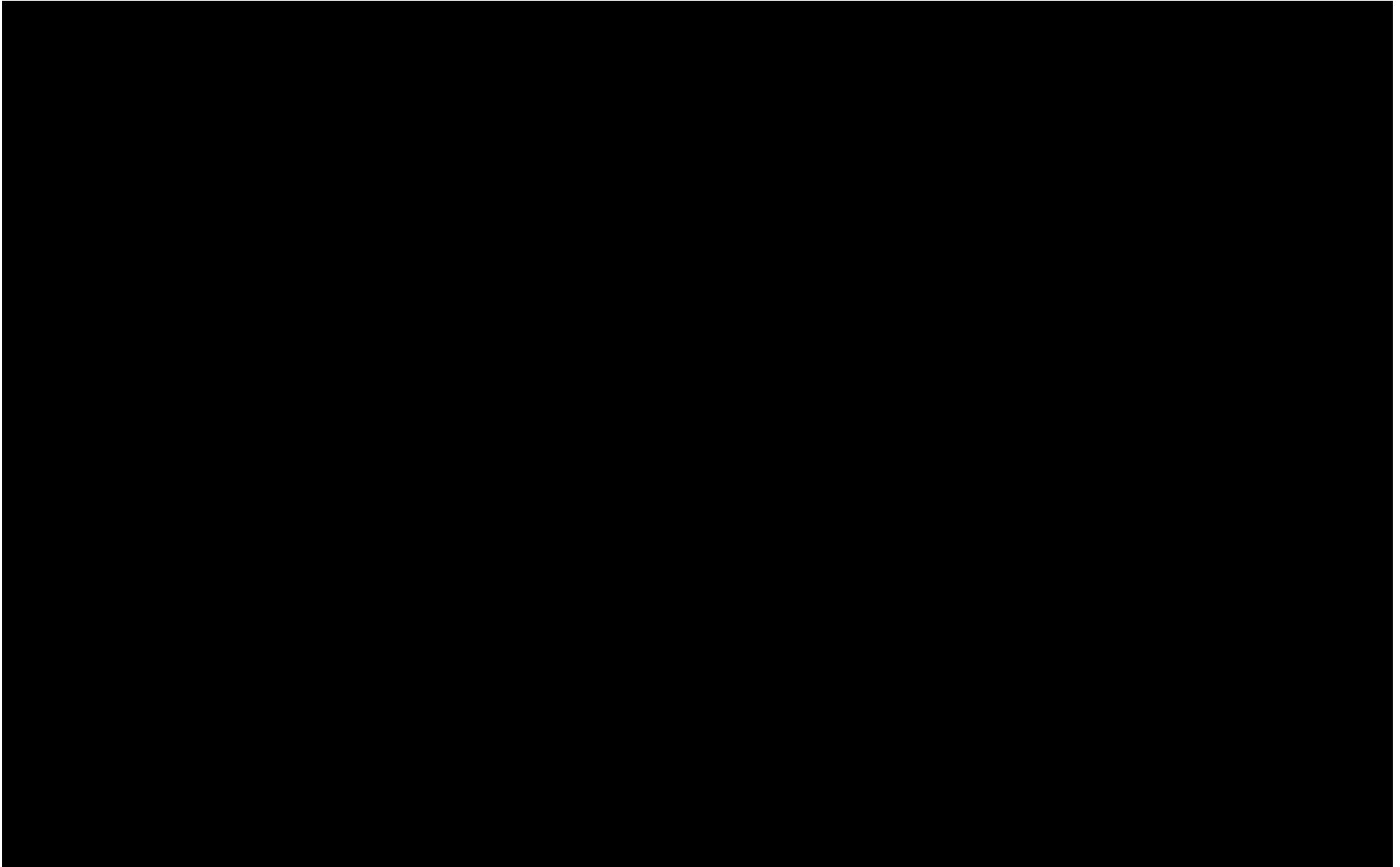


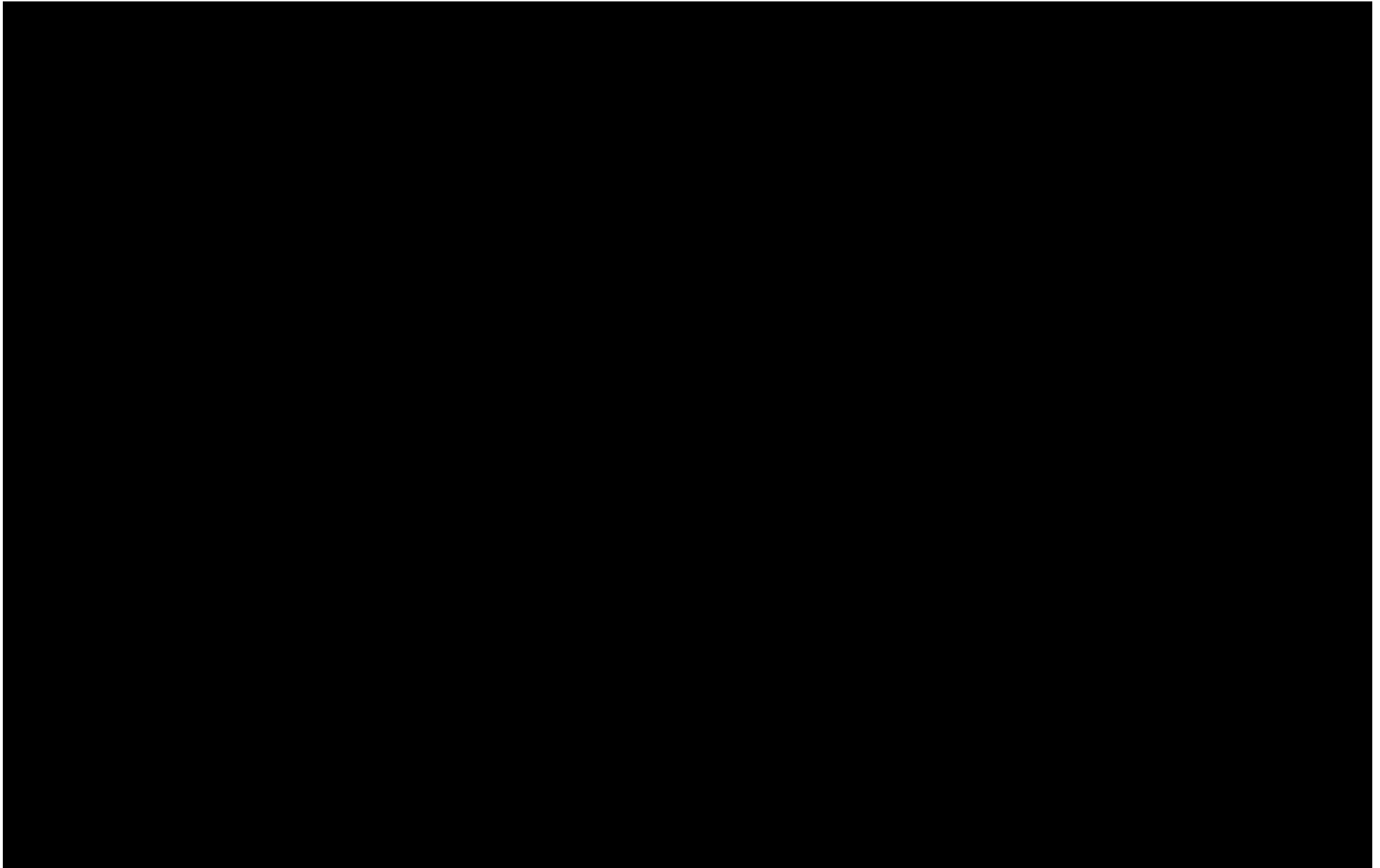
B. O&M Staffing Plan



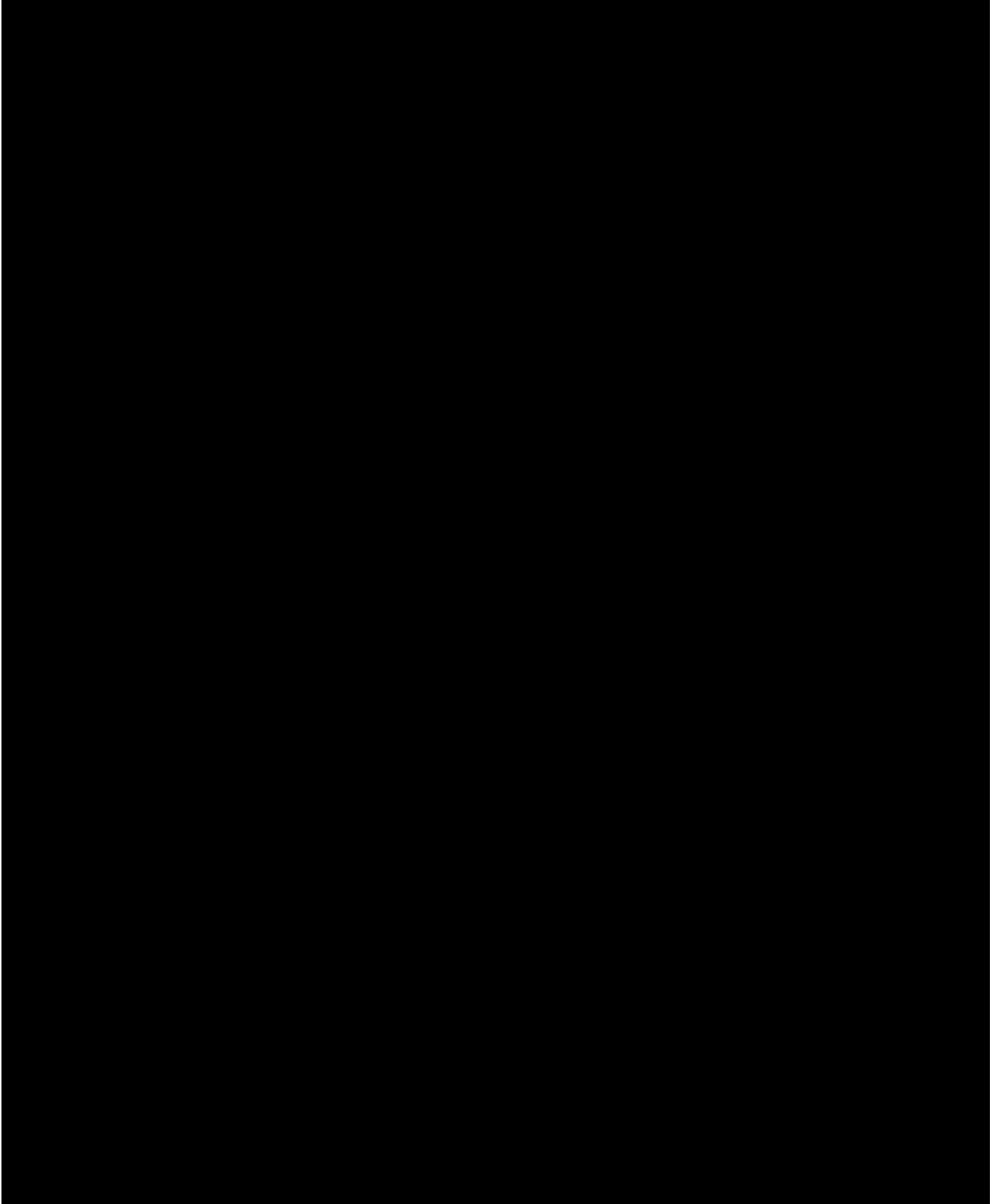


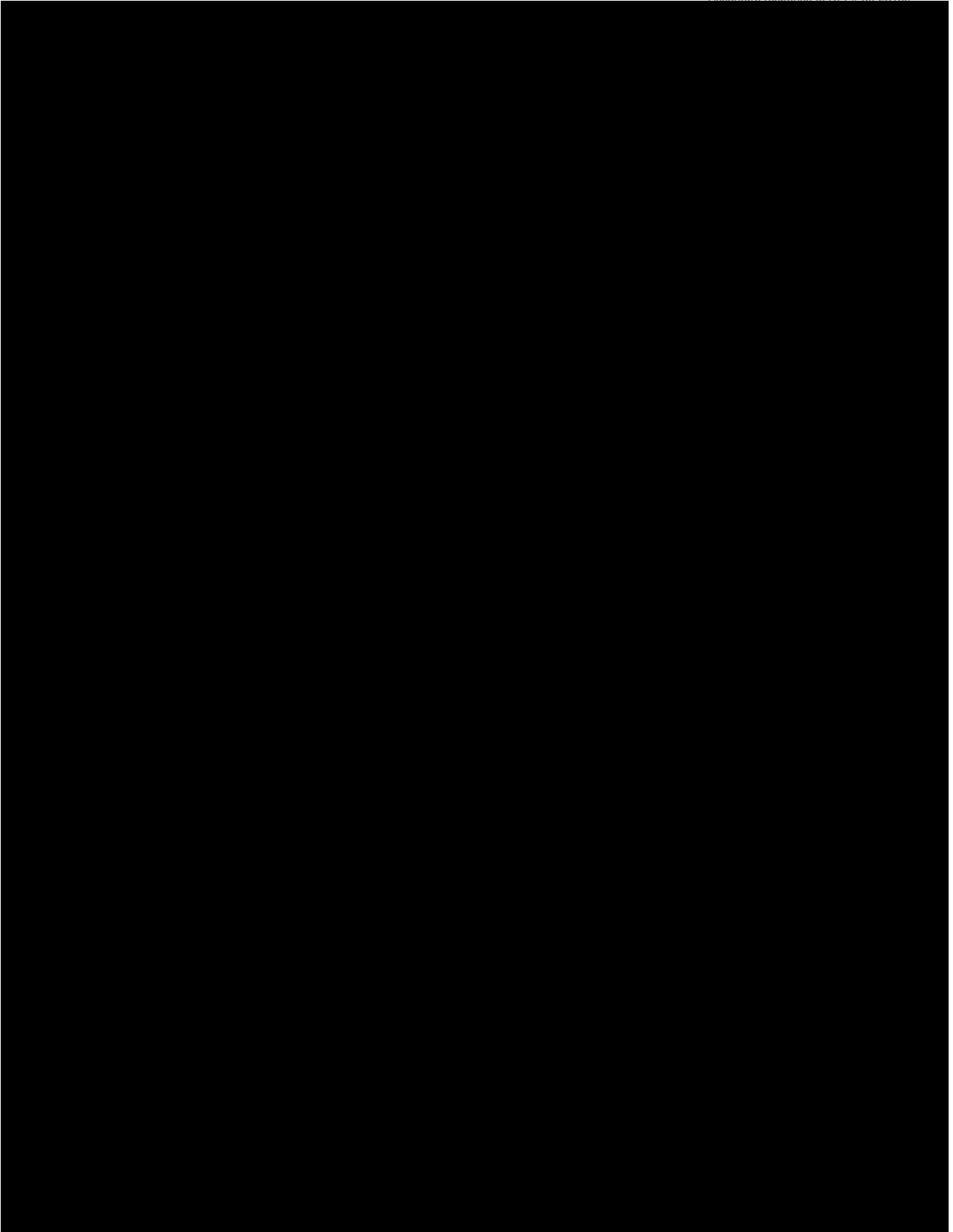


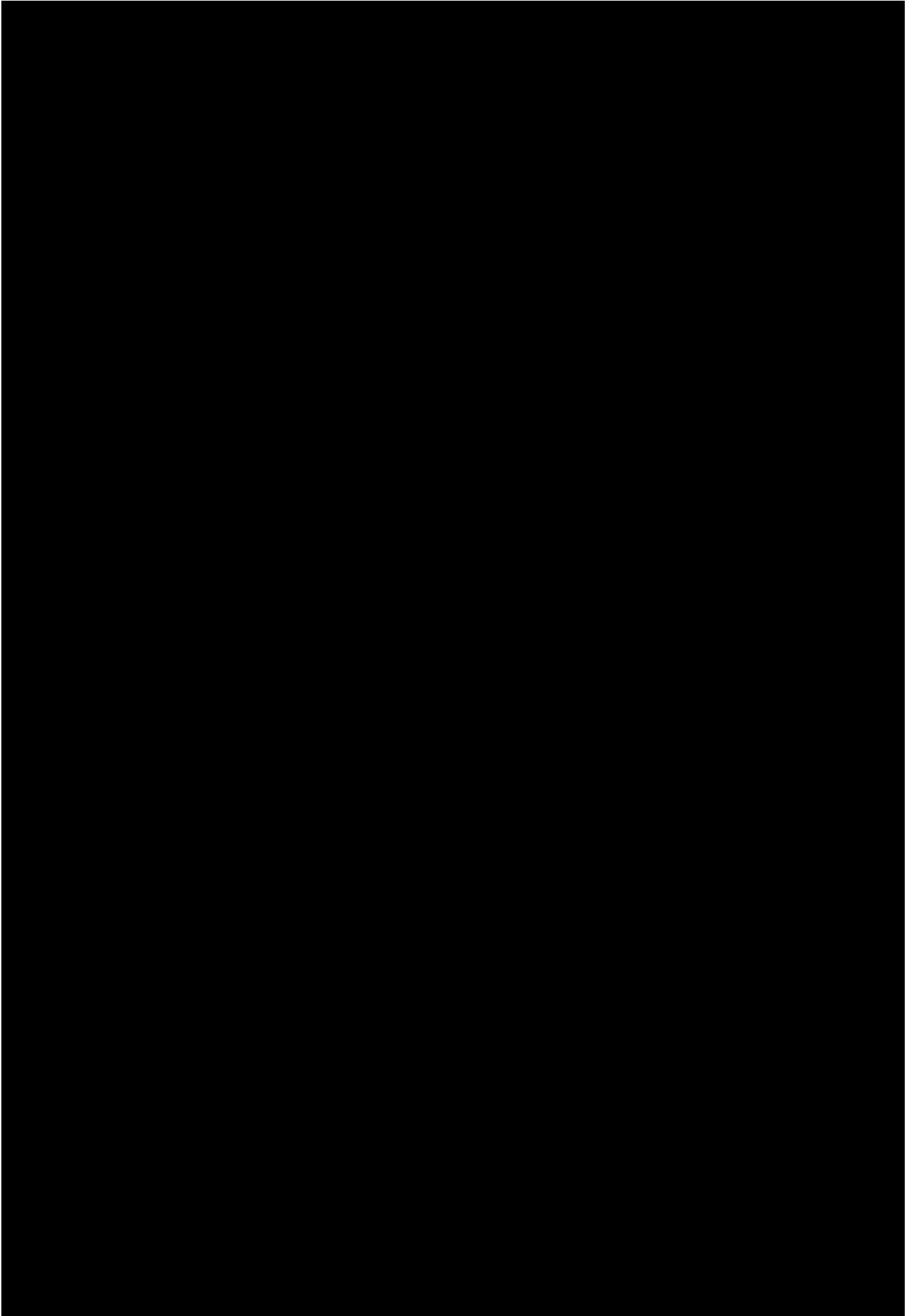


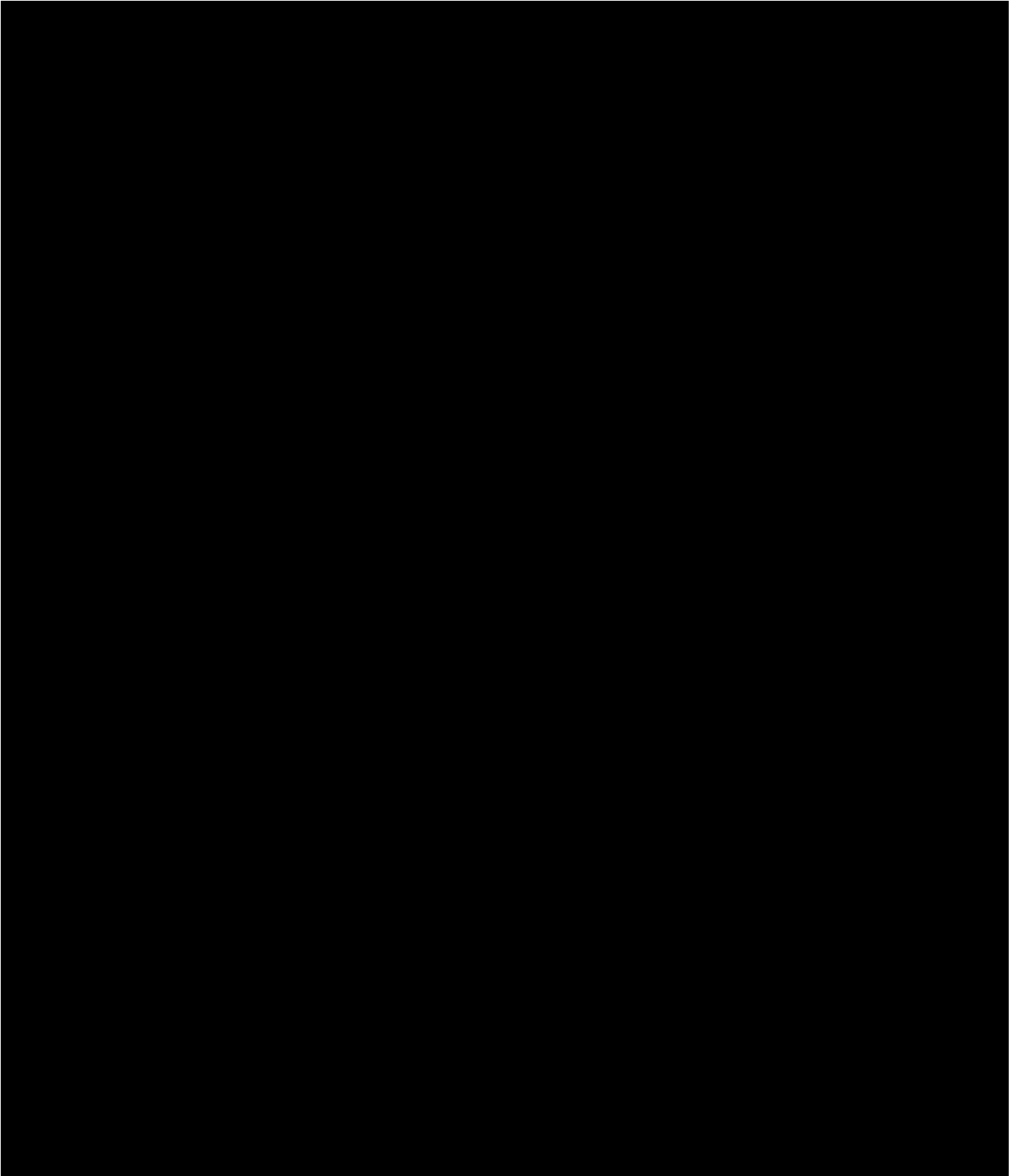


C. O&M Matrix of required skills/roles for each resource, O&M Roles and Responsibilities (and required skills for NCDHHS roles)

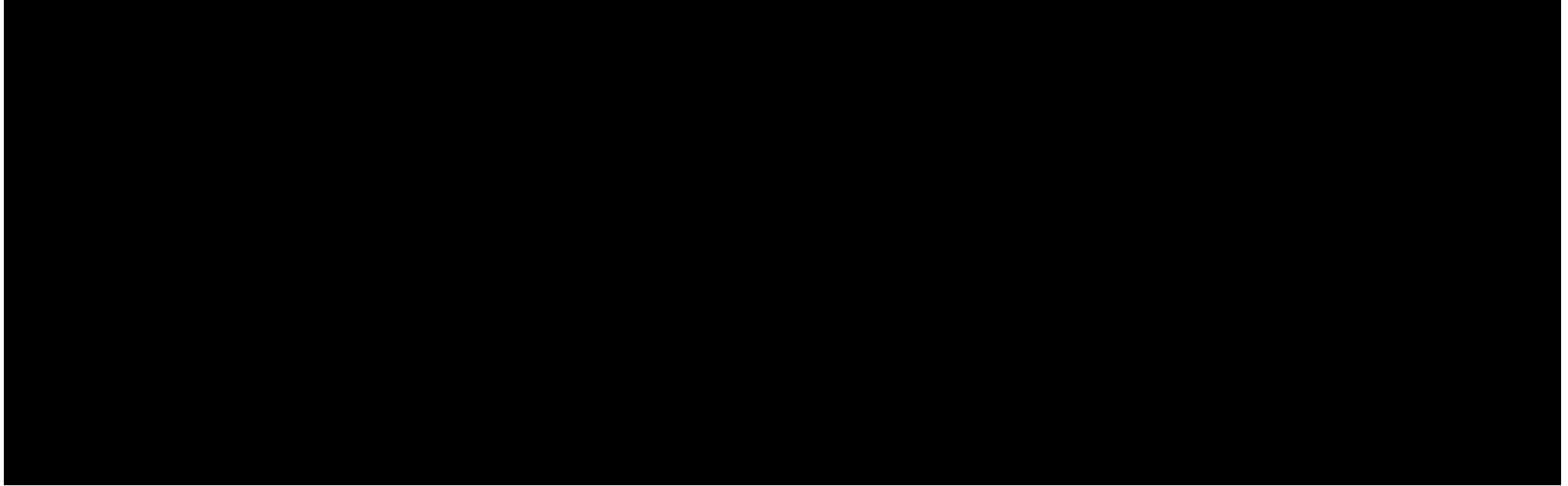






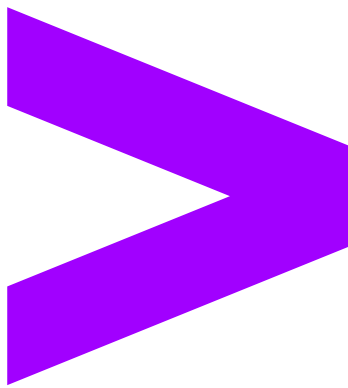


E. O&M Organization Chart



F. O&M Other resources available to the Agency

To be completed at project startup.



Copyright © 2023 Accenture
All rights reserved.
Accenture and its logo are trademarks of Accenture.