DS

PROFESSIONAL SERVICES CONTRACT

Contract #00000000000000000000079743

This Contract ("Contract"), entered into by and between Indiana Office of Technology (the "State") and Indiana Interactive, LLC dba Tyler Indiana (the "Contractor"), is executed pursuant to the terms and conditions set forth herein. In consideration of those mutual undertakings and covenants, the parties agree as follows:

1. Duties of Contractor. The Contractor shall provide the following services relative to this Contract: The Contractor shall provide the services necessary to maintain and operate the State Web Portal (IN.gov) to continue operations as they stand today and expand such services to meet future needs. The Contractor shall provide operations management, including datacenter hosting, website production, and outward facing web-based application development. The Contractor shall also provide executive oversight, business analysis, project management, design, development, quality assurance, security monitoring, and customer service in support of the IN.gov program.

Scope of Work requirements are set forth in **Exhibit 1.** Service Level Agreements are set forth in **Exhibit 3.** Software as a Service (SaaS) terms and conditions are set forth in **Exhibit 4.** Exhibits 1-4 are attached and incorporated fully into this Contract. The Contractor's implementation plan is set forth in **Exhibit 5**. The Contractor's plans to innovate the IN.gov Web Portal are set forth in **Exhibit 6**. The Contractor's disaster recovery plans are set forth in **Exhibit 7**. The Contractor's plans for responding to a privacy incident are set forth in **Exhibit 8**. The Contractor's staffing plans, and staff organization chart are set forth in **Exhibit 9** and **Exhibit 10**. The Contractor's issue priority level matrix is set forth in **Exhibit 11**. The Contractor's internal accessibility policy is set forth in **Exhibit 12**. A redacted version of Exhibits 5-12 are attached and incorporated by reference into this Contract.

2. Consideration. Pricing and associated terms and conditions are set forth in **Exhibit 2**, attached hereto and incorporated herein. Total remuneration under this Contract shall not exceed $22,715,850.00.

3. Term. This Contract shall be effective for a period of four (4) years. It shall commence on October 25, 2024 and shall remain in effect through October 24, 2028. There may be two (2) two-year renewals for a total of eight (8) years at the State's option.

4. Access to Records. The Contractor and its subcontractors, if any, shall maintain all books, documents, papers, accounting records, and other evidence pertaining to all costs incurred under this Contract. They shall make such materials available at their respective offices at all reasonable times during this Contract, and for three (3) years from the date of final payment under this Contract, for inspection by the State or its authorized designees. Copies shall be furnished at no cost to the State if requested. The access to records shall be upon no less than 10 business days' advance written notice and shall be no more often than once per calendar year.

5. Assignment; Successors.
A. The Contractor binds its successors and assignees to all the terms and conditions of this Contract. The Contractor may assign its right to receive payments to such third parties as the Contractor may desire without the prior written consent of the State, provided that the Contractor gives written notice (including evidence of such assignment) to the State thirty (30) days in advance of any payment so assigned. The assignment shall cover all unpaid amounts under this Contract and shall not be made to more than one party.

B. The Contractor shall not assign or subcontract the whole or any part of this Contract without the State's prior written consent. Additionally, the Contractor shall provide prompt written notice to the State of any change in the Contractor's legal name or legal status so that the changes may be documented and payments to the successor entity may be made.

6. Assignment of Antitrust Claims. As part of the consideration for the award of this Contract, the Contractor assigns to the State all right, title and interest in and to any claims the Contractor now has, or may acquire, under state or federal antitrust laws relating to the products or services which are the subject of this Contract.

7. Audits. The Contractor acknowledges that it may be required to submit to an audit of funds paid through this Contract. Any such audit shall be conducted in accordance with IC § 5-11-1, *et seq.*, and audit guidelines specified by the State.

The State considers the Contractor to be a "Contractor" under 2 C.F.R. 200.331 for purposes of this Contract. However, if it is determined that the Contractor is a "subrecipient" and if required by applicable provisions of 2 C.F.R. 200 (Uniform Administrative Requirements, Cost Principles, and Audit Requirements), Contractor shall arrange for a financial and compliance audit, which complies with 2 C.F.R. 200.500 *et seq*. The audit shall be upon no less than 10 business days' advance written notice and shall be no more often than once per calendar year.

8. Authority to Bind Contractor. The signatory for the Contractor represents that he/she has been duly authorized to execute this Contract on behalf of the Contractor and has obtained all necessary or applicable approvals to make this Contract fully binding upon the Contractor when his/her signature is affixed, and accepted by the State.

9. Changes in Work. The Contractor shall not commence any additional work or change the scope of the work until authorized in writing by the State. The Contractor shall make no claim for additional compensation in the absence of a prior written approval and amendment executed by all signatories hereto. This Contract may only be amended, supplemented or modified by a written document executed in the same manner as this Contract.

10. Compliance with Laws.
A. The Contractor shall comply with all applicable federal, state, and local laws, rules, regulations, and ordinances, and all provisions required thereby to be included herein are hereby incorporated by reference. The enactment or modification of any applicable state or federal statute or the promulgation of rules or regulations thereunder after execution of this Contract shall be reviewed by the State and the Contractor to determine whether the provisions of this Contract require formal modification.

B. The Contractor and its agents shall abide by all ethical requirements that apply to persons who have a business relationship with the State as set forth in IC § 4-2-6, *et seq*., IC § 4-2-7, *et seq*. and the regulations promulgated thereunder. **If the Contractor has knowledge, or would have acquired knowledge with reasonable inquiry, that a state officer, employee, or special state appointee, as those terms are defined in IC § 4-2-6-1, has a financial interest in the Contract, the Contractor shall ensure compliance with the disclosure requirements in IC § 4-2-6-10.5 prior to the execution of this Contract.** If the Contractor is not familiar with these ethical requirements, the Contractor should refer any questions to the Indiana State Ethics

Commission, or visit the Inspector General's website at http://www.in.gov/ig/. If the Contractor or its agents violate any applicable ethical standards, the State may, in its sole discretion, terminate this Contract immediately upon notice to the Contractor. In addition, the Contractor may be subject to penalties under IC §§ 4-2-6, 4-2-7, 35-44.1-1-4, and under any other applicable laws.

C. The Contractor certifies by entering into this Contract that neither it nor its principal(s) is presently in arrears in payment of taxes, permit fees or other statutory, regulatory or judicially required payments to the State of Indiana. The Contractor agrees that any payments currently due to the State of Indiana may be withheld from payments due to the Contractor. Additionally, further work or payments may be withheld, delayed, or denied and/or this Contract suspended until the Contractor is current in its payments and has submitted proof of such payment to the State.

D. The Contractor warrants that it has no current, pending or outstanding criminal, civil, or enforcement actions initiated by the State, and agrees that it will immediately notify the State of any such actions. During the term of such actions, the Contractor agrees that the State may delay, withhold, or deny work under any supplement, amendment, change order or other contractual device issued pursuant to this Contract.

E. If a valid dispute exists as to the Contractor's liability or guilt in any action initiated by the State or its agencies, and the State decides to delay, withhold, or deny work to the Contractor, the Contractor may request that it be allowed to continue, or receive work, without delay. The Contractor must submit, in writing, a request for review to the Indiana Department of Administration (IDOA) following the procedures for disputes outlined herein. A determination by IDOA shall be binding on the parties. Any payments that the State may delay, withhold, deny, or apply under this section shall not be subject to penalty or interest, except as permitted by IC § 5-17-5.

F. The Contractor warrants that the Contractor and its subcontractors, if any, shall obtain and maintain all required permits, licenses, registrations, and approvals, and shall comply with all health, safety, and environmental statutes, rules, or regulations in the performance of work activities for the State. Failure to do so may be deemed a material breach of this Contract and grounds for immediate termination and denial of further work with the State.

G. The Contractor affirms that, if it is an entity described in IC Title 23, it is properly registered and owes no outstanding reports to the Indiana Secretary of State.

H. As required by IC § 5-22-3-7:

(1) The Contractor and any principals of the Contractor certify that:

(A) the Contractor, except for de minimis and nonsystematic violations, has not violated the terms of:

(i) IC §24-4.7 [Telephone Solicitation Of Consumers];

(ii) IC §24-5-12 [Telephone Solicitations]; or

(iii) IC §24-5-14 [Regulation of Automatic Dialing Machines];

in the previous three hundred sixty-five (365) days, even if IC § 24-4.7 is preempted by federal law; and

(B) the Contractor will not violate the terms of IC § 24-4.7 for the duration of the Contract, even if IC §24-4.7 is preempted by federal law.

(2) The Contractor and any principals of the Contractor certify that an affiliate or principal of the Contractor and any agent acting on behalf of the Contractor or on behalf of an affiliate or principal of the Contractor, except for de minimis and nonsystematic violations,

(A) has not violated the terms of IC § 24-4.7 in the previous three hundred sixty-five (365) days, even if IC §24-4.7 is preempted by federal law; and

(B) will not violate the terms of IC § 24-4.7 for the duration of the Contract, even if IC §24-4.7 is preempted by federal law.

11. Condition of Payment. All services provided by the Contractor under this Contract must be performed in accordance with the functional specifications or other warranted functionality called for in the Contract and related documents (including SLAs), as determined at the good faith discretion of the undersigned State representative and in accordance with all applicable federal, state, local laws, ordinances, rules and regulations. The State shall not be required to pay for work found to be outside of this standard or otherwise inconsistent with this Contract or performed in violation of any federal, state or local statute, ordinance, rule or regulation.

12. Confidentiality of Information.

A. State Information
The Contractor understands and agrees that data, materials, and information disclosed to the Contractor may contain confidential and protected information. The Contractor covenants that data, material, and information gathered, based upon or disclosed to the Contractor for the purpose of this Contract will not be disclosed to or discussed with third parties without the prior written consent of the State.

The parties acknowledge that the services to be performed by Contractor for the State under this Contract may require or allow access to data, materials, and information containing Social Security numbers maintained by the State in its computer system or other records. In addition to the covenant made above in this section and pursuant to 10 IAC 5-3-1(4), the Contractor and the State agree to comply with the provisions of IC § 4-1-10 and IC § 4-1-11. If any Social Security number(s) is/are disclosed by Contractor, Contractor agrees to pay the cost of the notice of disclosure of a breach of the security of the system in addition to any other claims and expenses for which it is liable under the terms of this contract.

B. Contractor Information
For the purposes of this paragraph 12.B., - and only to the extent not inconsistent with Indiana law - "confidential and proprietary information" shall include the following:

1. All books, records, documents, and electronic files that pertain to the business or operation of the Contractor's company or that of its corporate parent, affiliates, or subsidiaries unless the same are disclosed publicly by Contractor or its corporate parent, affiliates, or subsidiaries.
2. The Software. "Software" is defined as all software (including documentation, source code, object code, and updates) developed by Contractor, or one of its affiliates, and deployed for this contract (excluding third-party software and excluding Contractor Software-as-a-Service "SaaS" services, and any other services provided by an affiliate, which is owned by an affiliate, together with any software updates or upgrades made by Contractor under this Contract.
3. Any Contractor "Trade Secret" as the term is defined under Indiana law. For illustrative purposes, trade secrets are information which derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertained through proper means by, other persons who can obtain economic value from its disclosure or use. Among other things, Trade Secrets include, but are not limited to, details about Contractor's product designs, application programming interfaces (APIs), or other gateway integrations.

The State covenants that Contractor Confidential Information will not be disclosed to or discussed with third parties without the prior written consent of the Contractor.

With the exception of the Software and third-party software, which shall be automatically deemed confidential and proprietary information, when Contractor furnishes or discloses information deemed to be confidential or proprietary information, intangible form or verbally, it shall clearly mark or otherwise identify the information in a manner to indicate that it is considered by the Contractor to be confidential or proprietary information.

Notwithstanding any of the foregoing, the parties acknowledge that Indiana's Access to Public Records Act, IC 5-14-3, controls disclosure of any public record as that term is defined in such Act. Any such other records subject to a request for disclosure under Indiana's Access to Public Records Act will be reviewed in light of the exemptions from disclosure and disclosed only as required by the Act. Subject to the foregoing, it shall not be a violation of the Contract for the Contractor or the State to make any disclosure which (i) it reasonably believes is required by law, including in response to a subpoena or other court or governmental order, (ii) required for the enforcement of this Contract, (iii) as necessary for a party to defend any claims brought against it or (iv) permitted by applicable law, including but not limited to Indiana Code. Unless prohibited by applicable law, the receiving party will give the disclosing ten days' written notice and an opportunity to object to any such disclosure or production, if practicable.

13. Continuity of Services.

A. The Contractor recognizes that the service(s) to be performed under this Contract are vital to the State and must be continued without interruption and that, upon Contract expiration, a successor, either the State or another contractor, may continue them. The Contractor agrees to:

1. Furnish phase-in training; and
2. Exercise its best efforts and cooperation to effect an orderly and efficient transition to a successor.

B. The Contractor shall, upon the State's written notice:

1. Furnish phase-in, phase-out services for up to sixty (60) days after this Contract expires; and
2. Negotiate in good faith a plan with a successor to determine the nature and extent of phase-in, phase-out services required. The plan shall specify a training program and a date for transferring responsibilities for each division of work described in the plan, and shall be subject to the State's approval. The Contractor shall provide sufficient experienced personnel during the phase-in, phase-out period to ensure that the services called for by this Contract are maintained at the required level of proficiency.

C. Reserved.

D. The Contractor shall be reimbursed for all reasonable phase-in, phase-out costs (i.e., costs incurred within the agreed period after contract expiration that result from phase-in, phase-out operations).

14. Debarment and Suspension.

A. The Contractor certifies by entering into this Contract that neither it nor its principals nor any of its subcontractors are presently debarred, suspended, proposed for debarment, declared ineligible or voluntarily excluded from entering into this Contract by any federal agency or by any department, agency or political subdivision of the State of Indiana. The term "principal" for purposes of this Contract means an officer, director, owner, partner, key employee or other person with primary management or supervisory responsibilities, or a person who has a critical influence on or substantive control over the operations of the Contractor.

B. The Contractor certifies that it has verified the state and federal suspension and debarment status for all subcontractors receiving funds under this Contract and shall be solely responsible for any recoupment, penalties or costs that might arise from use of a suspended or debarred subcontractor. The Contractor shall immediately notify the State if any subcontractor becomes debarred or suspended, and shall, at the State's request, take all steps required by the State to

terminate its contractual relationship with the subcontractor for work to be performed under this Contract.

15. Default by State. If the State, sixty (60) days after receipt of written notice, fails to correct or cure any material breach of this Contract, the Contractor may cancel and terminate this Contract and institute measures to collect monies due up to and including the date of termination.

16. Disputes.
A. Should any disputes arise with respect to this Contract, the Contractor and the State agree to act immediately to resolve such disputes. Time is of the essence in the resolution of disputes.

B. The Contractor agrees that, the existence of a dispute notwithstanding, it will continue without delay to carry out all of its responsibilities under this Contract that are not affected by the dispute. Should the Contractor fail to continue to perform its responsibilities regarding all non-disputed work, without delay, any additional costs incurred by the State or the Contractor as a result of such failure to proceed shall be borne by the Contractor, and the Contractor shall make no claim against the State for such costs.

C. If the parties are unable to resolve a contract dispute between them after good faith attempts to do so, a dissatisfied party shall submit the dispute to the Commissioner of the Indiana Department of Administration for resolution. The dissatisfied party shall give written notice to the Commissioner and the other party. The notice shall include: (1) a description of the disputed issues, (2) the efforts made to resolve the dispute, and (3) a proposed resolution. The Commissioner shall promptly issue a Notice setting out documents and materials to be submitted to the Commissioner in order to resolve the dispute; the Notice may also afford the parties the opportunity to make presentations and enter into further negotiations. Within thirty (30) business days of the conclusion of the final presentations, the Commissioner shall issue a written decision and furnish it to both parties. The Commissioner's decision shall be the final and conclusive administrative decision unless either party serves on the Commissioner and the other party, within ten (10) business days after receipt of the Commissioner's decision, a written request for reconsideration and modification of the written decision. If the Commissioner does not modify the written decision within thirty (30) business days, either party may take such other action helpful to resolving the dispute, including submitting the dispute to an Indiana court of competent jurisdiction. If the parties accept the Commissioner's decision, it may be memorialized as a written Amendment to this Contract if appropriate.

D. The State may withhold payments on disputed items pending resolution of the dispute. The unintentional nonpayment by the State to the Contractor of one or more invoices not in dispute in accordance with the terms of this Contract will not be cause for the Contractor to terminate this Contract, and the Contractor may bring suit to collect these amounts without following the disputes procedure contained herein.

E. With the written approval of the Commissioner of the Indiana Department of Administration, the parties may agree to forego the process described in subdivision C. relating to submission of the dispute to the Commissioner.

F. This paragraph shall not be construed to abrogate provisions of IC § 4-6-2-11 in situations where dispute resolution efforts lead to a compromise of claims in favor of the State as described in that statute. In particular, releases or settlement agreements involving releases of legal claims or potential legal claims of the state should be processed consistent with IC § 4-6-2-11, which requires approval of the Governor and Attorney General.

17. Drug-Free Workplace Certification. As required by Executive Order No. 90-5 dated April 12, 1990, issued by the Governor of Indiana, the Contractor hereby covenants and agrees to make a good faith effort to provide and maintain a drug-free workplace. The Contractor will give written notice to the State within ten (10) days after receiving actual notice that the Contractor, or

an employee of the Contractor in the State of Indiana, has been convicted of a criminal drug violation occurring in the workplace. False certification or violation of this certification may result in sanctions including, but not limited to, suspension of contract payments, termination of this Contract and/or debarment of contracting opportunities with the State for up to three (3) years.

In addition to the provisions of the above paragraph, if the total amount set forth in this Contract is in excess of $25,000.00, the Contractor certifies and agrees that it will provide a drug-free workplace by:

A. Publishing and providing to all of its employees a statement notifying them that the unlawful manufacture, distribution, dispensing, possession or use of a controlled substance is prohibited in the Contractor's workplace, and specifying the actions that will be taken against employees for violations of such prohibition;

B. Establishing a drug-free awareness program to inform its employees of: (1) the dangers of drug abuse in the workplace; (2) the Contractor's policy of maintaining a drug-free workplace; (3) any available drug counseling, rehabilitation and employee assistance programs; and (4) the penalties that may be imposed upon an employee for drug abuse violations occurring in the workplace;

C. Notifying all employees in the statement required by subparagraph (A) above that as a condition of continued employment, the employee will: (1) abide by the terms of the statement; and (2) notify the Contractor of any criminal drug statute conviction for a violation occurring in the workplace no later than five (5) days after such conviction;

D. Notifying the State in writing within ten (10) days after receiving notice from an employee under subdivision (C)(2) above, or otherwise receiving actual notice of such conviction;

E. Within thirty (30) days after receiving notice under subdivision (C)(2) above of a conviction, imposing the following sanctions or remedial measures on any employee who is convicted of drug abuse violations occurring in the workplace: (1) taking appropriate personnel action against the employee, up to and including termination; or (2) requiring such employee to satisfactorily participate in a drug abuse assistance or rehabilitation program approved for such purposes by a federal, state or local health, law enforcement, or other appropriate agency; and

F. Making a good faith effort to maintain a drug-free workplace through the implementation of subparagraphs (A) through (E) above.

18. Employment Eligibility Verification. As required by IC § 22-5-1.7, the Contractor swears or affirms under the penalties of perjury that the Contractor does not knowingly employ an unauthorized alien. The Contractor further agrees that:

A. The Contractor shall enroll in and verify the work eligibility status of all his/her/its newly hired employees through the E-Verify program as defined in IC § 22-5-1.7-3. The Contractor is not required to participate should the E-Verify program cease to exist. Additionally, the Contractor is not required to participate if the Contractor is self-employed and does not employ any employees.

B. The Contractor shall not knowingly employ or contract with an unauthorized alien. The Contractor shall not retain an employee or contract with a person that the Contractor subsequently learns is an unauthorized alien.

C. The Contractor shall require his/her/its subcontractors, who perform work under this Contract, to certify to the Contractor that the subcontractor does not knowingly employ or contract with an unauthorized alien and that the subcontractor has enrolled and is participating in the E-Verify

program. The Contractor agrees to maintain this certification throughout the duration of the term of a contract with a subcontractor.

The State may terminate for default if the Contractor fails to cure a breach of this provision no later than thirty (30) days after being notified by the State.

19. Employment Option. Reserved.

20. Force Majeure. In the event that either party is unable to perform any of its obligations under this Contract or to enjoy any of its benefits because of natural disaster or decrees of governmental bodies not the fault of the affected party (hereinafter referred to as a "Force Majeure Event"), the party who has been so affected shall immediately or as soon as is reasonably possible under the circumstances give notice to the other party and shall do everything possible to resume performance. Upon receipt of such notice, all obligations under this Contract shall be immediately suspended. If the period of nonperformance exceeds thirty (30) days from the receipt of notice of the Force Majeure Event, the party whose ability to perform has not been so affected may, by giving written notice, terminate this Contract.

21. Funding Cancellation. As required by Financial Management Circular 3.3 and IC § 5-22-17-5, when the Director of the State Budget Agency makes a written determination that funds are not appropriated or otherwise available to support continuation of performance of this Contract, this Contract shall be canceled. A determination by the Director of State Budget Agency that funds are not appropriated or otherwise available to support continuation of performance shall be final and conclusive.

22. Governing Law. This Contract shall be governed, construed, and enforced in accordance with the laws of the State of Indiana, without regard to its conflict of laws rules. Suit, if any, must be brought in the State of Indiana.

23. HIPAA Compliance. If this Contract involves services, activities or products subject to the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Contractor covenants that it will appropriately safeguard Protected Health Information (defined in 45 CFR 160.103), and agrees that it is subject to, and shall comply with, the provisions of 45 CFR 164 Subpart E regarding use and disclosure of Protected Health Information.

24. Indemnification. The Contractor agrees to indemnify, defend, and hold harmless the State, its agents, officials, and employees from all third party claims and suits including court costs, attorney's fees, and other expenses caused by any act or omission of the Contractor and/or its subcontractors, if any, in the performance of this Contract. The State will not provide indemnification to the Contractor.

25. Independent Contractor; Workers' Compensation Insurance. The Contractor is performing as an independent entity under this Contract. No part of this Contract shall be construed to represent the creation of an employment, agency, partnership or joint venture agreement between the parties. Neither party will assume liability for any injury (including death) to any persons, or damage to any property, arising out of the acts or omissions of the agents, employees or subcontractors of the other party. The Contractor shall provide all necessary unemployment and workers' compensation insurance for the Contractor's employees, and Contractor shall provide the State with a Certificate of Insurance evidencing such coverage prior to starting work under this Contract.

26. Indiana Veteran Owned Small Business Enterprise Compliance. Award of this Contract was based, in part, on the Indiana Veteran Owned Small Business Enterprise ("IVOSB") participation plan, as detailed in the IVOSB Subcontractor Commitment Form, commonly referred to as "Attachment A-1" in the procurement documentation and incorporated by reference herein. Therefore, any changes to this information during the Contract term must be approved by

IDOA's Division of Supplier Diversity and may require an amendment. It is the State's expectation that the Contractor will meet the subcontractor commitments during the Contract term. ***The subcontractor commitment is based on Baseline Services only.***
The following certified IVOSB subcontractor(s) will be participating in this Contract:

IVOSB	COMPANY NAME	PHONE	EMAIL OF CONTACT PERSON	PERCENT
IVOSB	Bravia Services	(317) 590-3684	doug.heath@braviaservices.com	5%

Briefly describe the IVOSB service(s)/product(s) to be provided under this Contract and include the estimated date(s) for utilization during the Contract term:

Management and business professional and administrative services to facilitate Third-Party Portal Managed Applications under the contract.

A copy of each subcontractor agreement must be submitted to the Division of Supplier Diversity within thirty (30) days of the effective date of this Contract. The subcontractor agreements may be uploaded into Pay Audit (Indiana's subcontractor payment auditing system), emailed to IndianaVeteransPreference@idoa.IN.gov, or mailed to IDOA, 402 W. Washington Street, Room W-462, Indianapolis, IN 46204. Failure to provide a copy of any subcontractor agreement may be deemed a violation of the rules governing IVOSB procurement and may result in sanctions allowable under 25 IAC 9-5-2. Requests for changes must be submitted to IndianaVeteransPreference@idoa.IN.gov for review and approval before changing the participation plan submitted in connection with this Contract.

The Contractor shall report payments made to certified IVOSB subcontractors under this Contract on a monthly basis using Pay Audit. The Contractor shall notify subcontractors that they must confirm payments received from the Contractor in Pay Audit. The Pay Audit system can be accessed on the IDOA webpage at: www.in.gov/idoa/mwbe/payaudit.htm. The Contractor may also be required to report IVOSB certified subcontractor payments directly to the Division of Supplier Diversity, as reasonably requested and in the format required by the Division of Supplier Diversity.

The Contractor's failure to comply with the provisions in this clause may be considered a material breach of the Contract.

27. Information Technology Enterprise Architecture Requirements. If this Contract involves information technology-related products or services, the Contractor agrees that all such products or services are compatible with any of the technology standards found at https://www.in.gov/iot/2394.htm that are applicable, including the assistive technology standard. The State may terminate this Contract for default if the terms of this paragraph are breached.

28. Insurance.
A. The Contractor and its subcontractors (if any) shall secure and keep in force during the term of this Contract the following insurance coverages (if applicable) covering the Contractor for any and all claims of any nature which may in any manner arise out of or result from Contractor's performance under this Contract:

1. Commercial general liability, including contractual coverage, with policy limits of $1,000,000 per occurrence and $5,000,000 in the aggregate. The State is to be included as an additional insured on a primary, non-contributory basis for any liability arising directly or indirectly under or in connection with this Contract. The CGL limits may be met by a combination of the CGL policy and an Umbrella or Excess Liability policy.

2. Automobile liability for owned, non-owned and hired autos with policy limits of$1,000,000 combined single limit per accident for bodily injury and property damage. The State is to be included as an additional insured on a primary, non-contributory basis.

3. Technology Errors and Omissions or Cyber liability with a liability limit of $5,000,000 per claim and in the aggregate. Coverage for the benefit of the State shall continue for a period of two (2) years after the date of service provided under this Contract.

4. Intentionally omitted.

5. Intentionally omitted.

6. Intentionally omitted.

7. Intentionally omitted.

The Contractor shall provide proof of such insurance coverage by tendering to the undersigned State representative a certificate of insurance prior to the commencement of this Contract and proof of workers' compensation coverage meeting all statutory requirements of IC § 22-3-2. In addition, proof of an "all states endorsement" covering claims occurring outside the State is required if any of the services provided under this Contract involve work outside of Indiana.

B. The Contractor's insurance coverage must meet the following additional requirements:

1. The insurer must have a certificate of authority or other appropriate authorization to operate in the state in which the policy was issued.

2. Any deductible or self-insured retention amount or other similar obligation under the insurance policies shall be the sole obligation of the Contractor.

3. The duty of the Contractor to indemnify the State as required elsewhere under this Contract shall not be limited by the insurance required in this Contract.

4. Contractor shall not cancel or cause the insurance required in this Contract to be in reach of these requirements without Contractor providing thirty (30) days' prior written notice to the undersigned State agency (10 days for non-payment of premium).

5. The Contractor waives and agrees to require their insurer to waive their rights of subrogation against the State of Indiana for claims that arise out of the Contractor under the CGL and Automobile policies, except to the extent that the damage or loss was caused by the State.

C. Failure to provide insurance as required in this Contract may be deemed a material breach of contract entitling the State to terminate this Contract after the notice and cure period provided for herein. The Contractor shall furnish a certificate of insurance and all endorsements to the State before the commencement of this Contract.

29. Key Person(s).

A. If both parties have designated that certain individual(s) are essential to the services offered, the parties agree that should such individual(s) leave their employment during the term of this Contract for whatever reason, Contractor shall promptly replace such key person with an individual that is reasonably acceptable to the State.

B. In the event that the Contractor is an individual, that individual shall be considered a key person and, as such, essential to this Contract. Substitution of another for the Contractor shall not be permitted without express written consent of the State.

Nothing in sections A and B, above shall be construed to prevent the Contractor from using the services of others to perform tasks ancillary to those tasks which directly require the expertise of

the key person. Examples of such ancillary tasks include secretarial, clerical, and common labor duties. The Contractor shall, at all times, remain responsible for the performance of all necessary tasks, whether performed by a key person or others.

Key person(s) to this Contract is/are None.

30. Licensing Standards. The Contractor, its employees and subcontractors shall comply with all applicable licensing standards, certification standards, accrediting standards and any other laws, rules, or regulations governing services to be provided by the Contractor pursuant to this Contract. The State will not pay the Contractor for any services performed when the Contractor, its employees or subcontractors are not in compliance with such applicable standards, laws, rules, or regulations. If any license, certification or accreditation expires or is revoked, or any disciplinary action is taken against an applicable license, certification, or accreditation, the Contractor shall notify the State immediately and the State, at its option, may immediately terminate this Contract.

31. Merger & Modification. This Contract constitutes the entire agreement between the parties. No understandings, agreements, or representations, oral or written, not specified within this Contract will be valid provisions of this Contract. This Contract may not be modified, supplemented, or amended, except by written agreement signed by all necessary parties.

32. Minority and Women's Business Enterprises Compliance.
Award of this Contract was based, in part, on the Minority and/or Women's Business Enterprise ("MBE" and/or "WBE") participation plan as detailed in the Minority and Women's Business Enterprises Subcontractor Commitment Form, commonly referred to as "Attachment A" in the procurement documentation and incorporated by reference herein**.** Therefore, any changes to this information during the Contract term must be approved by Division of Supplier Diversity and may require an amendment. It is the State's expectation that the Contractor will meet the subcontractor commitments during the Contract term. ***The subcontractor commitment is based on Baseline Services only.***

The following Division of Supplier Diversity certified MBE and/or WBE subcontractors will be participating in this Contract:

MBE or WBE	COMPANY NAME	PHONE	EMAIL OF CONTACT PERSON	PERCENT
WBE	netlogx	(765) 721-3705	kriegel@netlogx.com	5%
WBE	Roeing IT Solutions	(765) 474-5402	sfey@roeing.com	3%
WBE	DSN	(844) 983-3444	nabil@dsnw orldwide.com	3%
MBE	Engaging Solutions LLC	(317) 918-2335	cmosby@engagingsolutions.net	8%

Briefly describe the MBE and/or WBE service(s)/product(s) to be provided under this Contract and include the estimated date(s) for utilization during the Contract term:
Project management and project coordination services to support project engagements.
Providing IT technology consultation services and IT services to support database administration and support tasks.
IT consulting and staffing services to support API and other development efforts.
Program compliance, training program consultation services and other operational needs to support report and SLA management, and training.

A copy of each subcontractor agreement must be submitted to the Division of Supplier Diversity within thirty (30) days of the effective date of this Contract. The subcontractor agreements may be uploaded into Pay Audit (Indiana's subcontractor payment auditing system), emailed to MWBECompliance@idoa.IN.gov, or mailed to Division of Supplier Diversity, 402 W. Washington Street, Room W-462, Indianapolis IN 46204. Failure to provide a copy of any subcontractor agreement may be deemed a violation of the rules governing MBE/WBE procurement and may result in sanctions allowable under 25 IAC 5-7-8. Requests for changes must be submitted to

MWBECompliance@idoa.IN.gov for review and approval before changing the participation plan submitted in connection with this Contract.

The Contractor shall report payments made to Division of Supplier Diversity certified subcontractors under this Contract on a monthly basis using Pay Audit. The Contractor shall notify subcontractors that they must confirm payments received from the Contractor in Pay Audit. The Pay Audit system can be accessed on the IDOA webpage at: www.in.gov/idoa/mwbe/payaudit.htm. The Contractor may also be required to report Division of Supplier Diversity certified subcontractor payments directly to the Division, as reasonably requested and in the format required by the Division of Supplier Diversity.

The Contractor's failure to comply with the provisions in this clause may be considered a material breach of the Contract.

33. Nondiscrimination. Pursuant to the Indiana Civil Rights Law, specifically IC § 22-9-1-10, and in keeping with the purposes of the federal Civil Rights Act of 1964, the Age Discrimination in Employment Act, and the Americans with Disabilities Act, the Contractor covenants that it shall not discriminate against any employee or applicant for employment relating to this Contract with respect to the hire, tenure, terms, conditions or privileges of employment or any matter directly or indirectly related to employment, because of the employee's or applicant's race, color, national origin, religion, sex, age, disability, ancestry, status as a veteran, or any other characteristic protected by federal, state, or local law ("Protected Characteristics"). The Contractor certifies compliance with applicable federal laws, regulations, and executive orders prohibiting discrimination based on the Protected Characteristics in the provision of services. Breach of this paragraph may be regarded as a material breach of this Contract, but nothing in this paragraph shall be construed to imply or establish an employment relationship between the State and any applicant or employee of the Contractor or any subcontractor.

The State is a recipient of federal funds, and therefore, where applicable, the Contractor and any subcontractors shall comply with requisite affirmative action requirements, including reporting, pursuant to 41 CFR Chapter 60, as amended, and Section 202 of Executive Order 11246 as amended by Executive Order 13672.

34. Notice to Parties. Whenever any notice, statement or other communication is required under this Contract, it will be sent by E-mail or first-class U.S. mail service to the following addresses, unless otherwise specifically advised.

A. Notices to the State shall be sent to:

Indiana Office of Technology
Michael White
100 N Senate Avenue
Indianapolis, IN 46204
E-mail: mwhite1@iot.in.gov

B. Notices to the Contractor shall be sent to:

Indiana Interactive dba Tyler Indiana
Andrew Hoff
151 W. Ohio Street, Suite 100
Indianapolis, IN 46204
E-mail: andrew.hoff@tylertech.com

As required by IC § 4-13-2-14.8, payments to the Contractor shall be made via electronic funds transfer in accordance with instructions filed by the Contractor with the Indiana Auditor of State.

35. Order of Precedence; Incorporation by Reference. Any inconsistency or ambiguity in this Contract shall be resolved by giving precedence in the following order: (1) this Contract, (2) attachments prepared by the State, (3) RFP #23-74658 (4) Contractor's response to RFP #23-74658, and (5) attachments prepared by the Contractor. All attachments, and all documents referred to in this paragraph, are hereby incorporated fully by reference.

36. Ownership of Documents and Materials.
A. All documents, records, programs, applications, data, algorithms, film, tape, articles, memoranda, and other materials (the "Materials") not developed or licensed by the Contractor prior to execution of this Contract, but specifically developed under this Contract shall be considered "work for hire" and the Contractor hereby transfers and assigns any ownership claims to the State so that all Materials will be the property of the State. If ownership interest in the Materials cannot be assigned to the State, the Contractor grants the State a non-exclusive, non-cancelable, perpetual, worldwide royalty-free license to use the Materials and to use, modify, copy and create derivative works of the Materials.

B. Use of the Materials, other than related to contract performance by the Contractor, without the prior written consent of the State, is prohibited. During the performance of this Contract, the Contractor shall be responsible for any loss of or damage to the Materials developed for or supplied by the State and used to develop or assist in the services provided while the Materials are in the possession of the Contractor. Any loss or damage thereto shall be restored at the Contractor's expense. The Contractor shall provide the State full, immediate, and unrestricted access to the Materials and to Contractor's work product during the term of this Contract.

37. Payments.
A. All payments shall be made thirty five (35) days in arrears in conformance with State fiscal policies and procedures and, as required by IC §4-13-2-14.8, the direct deposit by electronic funds transfer to the financial institution designated by the Contractor in writing unless a specific waiver has been obtained from the Indiana Auditor of State. No payments will be made in advance of receipt of the goods or services that are the subject of this Contract except as permitted by IC § 4-13-2-20.

B. If the Contractor is being paid in advance for the maintenance of equipment, software or a service as a subscription, then pursuant to IC § 4-13-2-20(b)(14), the Contractor agrees that if it fails to fully provide or perform under this Contract, upon receipt of written notice from the State, it shall promptly refund the consideration paid, pro-rated through the date of non-performance.

38. Penalties/Interest/Attorney's Fees. The State will in good faith perform its required obligations hereunder and does not agree to pay any penalties, liquidated damages, interest or attorney's fees, except as permitted by Indiana law, in part, IC § 5-17-5, IC § 34-54-8, IC § 34-13-1 and IC § 34-52-2.

Notwithstanding the provisions contained in IC § 5-17-5, any liability resulting from the State's failure to make prompt payment shall be based solely on the amount of funding originating from the State and shall not be based on funding from federal or other sources.

39. Progress Reports. The Contractor shall submit progress reports to the State upon request. The report shall be oral, unless the State, upon receipt of the oral report, should deem it necessary to have it in written form. The progress reports shall serve the purpose of assuring the State that work is progressing in line with the schedule, and that completion can be reasonably assured on the scheduled date.

40. Public Record. The Contractor acknowledges that the State will not treat this Contract as containing confidential information, and the State will post this Contract on the transparency

portal as required by Executive Order 05-07 and IC § 5-14-3.5-2. Use by the public of the information contained in this Contract shall not be considered an act of the State.

41. Renewal Option. This Contract may be renewed under the same terms and conditions, subject to the approval of the Commissioner of the Department of Administration and the State Budget Director in compliance with IC § 5-22-17-4. The term of the renewed contract may not be longer than the term of the original Contract.

42. Severability. The invalidity of any section, subsection, clause or provision of this Contract shall not affect the validity of the remaining sections, subsections, clauses or provisions of this Contract.

43. Substantial Performance. This Contract shall be deemed to be substantially performed only when fully performed according to its terms and conditions and any written amendments or supplements.

44. Taxes. The State is exempt from most state and local taxes and many federal taxes. The State will not be responsible for any taxes levied on the Contractor as a result of this Contract.

45. Termination for Convenience. This Contract may be terminated, in whole or in part, by the State, which shall include and is not limited to IDOA and the State Budget Agency whenever, for any reason, the State determines that such termination is in its best interest. Termination of services shall be effected by delivery to the Contractor of a Termination Notice at least thirty (30) days prior to the termination effective date, specifying the extent to which performance of services under such termination becomes effective. The Contractor shall be compensated for services properly rendered prior to the effective date of termination. The State will not be liable for services performed after the effective date of termination. The Contractor shall be compensated for services herein provided but in no case shall total payment made to the Contractor exceed the original contract price or shall any price increase be allowed on individual line items if canceled only in part prior to the original termination date. For the purposes of this paragraph, the parties stipulate and agree that IDOA shall be deemed to be a party to this Contract with authority to terminate the same for convenience when such termination is determined by the Commissioner of IDOA to be in the best interests of the State.

46. Termination for Default.

A. With the provision of thirty (30) days' notice to the Contractor, the State may terminate this Contract if the Contractor fails to cure any breach of this Contract; the time to correct or cure the breach may be extended beyond thirty (30) days if the State determines progress is being made and the extension is agreed to by the parties.

B. If the State terminates this Contract for an uncured default, it may acquire, under the terms and in the manner the State considers appropriate, supplies or services similar to those terminated, and the Contractor will be liable to the State for any excess costs for those supplies or services.

C. The State shall pay the contract price for completed supplies delivered and services accepted. The Contractor and the State shall agree on the amount of payment for manufacturing materials delivered and accepted and for the protection and preservation of the property. Failure to agree will be a dispute under the Disputes clause. The State may withhold from these amounts any sum the State determines to be necessary to protect the State against loss because of outstanding liens or claims of former lien holders.

D. The rights and remedies of the State in this clause are in addition to any other rights and remedies provided by law or equity or under this Contract.

47. Travel. No expenses for travel will be reimbursed unless specifically authorized by this Contract. Permitted expenses will be reimbursed at the rate paid by the State and in accordance with the *Indiana Department of Administration Travel Policy and Procedures* in effect at the time the expenditure is made. Out-of-state travel requests must be reviewed by the State for availability of funds and for conformance with *Travel Policy* guidelines.

48. Waiver of Rights. No right conferred on either party under this Contract shall be deemed waived, and no breach of this Contract excused, unless such waiver is in writing and signed by the party claimed to have waived such right. Neither the State's review, approval or acceptance of, nor payment for, the services required under this Contract shall be construed to operate as a waiver of any rights under this Contract or of any cause of action arising out of the performance of this Contract, and the Contractor shall be and remain liable to the State in accordance with applicable law for all damages to the State caused by the Contractor's negligent performance of any of the services furnished under this Contract.

49. Work Standards. The Contractor shall execute its responsibilities by following and applying at all times the highest professional and technical guidelines and standards. If the State becomes dissatisfied with the work product of or the working relationship with those individuals assigned to work on this Contract, the State may request in writing the replacement of any or all such individuals, and the Contractor shall grant such request.

50. State Boilerplate Affirmation Clause. I swear or affirm under the penalties of perjury that I have not altered, modified, changed or deleted the State's standard contract clauses (as contained in the *2022 SCM Template*) in any way except as follows:

4 Access to Records. Modified
7 Audits. Modified
11 Condition of Payment. Modified
12 Confidentiality of Information. Modified
13 Continuity of Services. Modified
19 Employment Option. Reserved
26 Indiana Veteran Owned Small Business Enterprise Compliance. Modified
28 Insurance. Modified
29 Key Persons. Modified
32 Minority and Women's Business Enterprise Compliance. Modified
34 Notice to Persons. Modified
46 Termination for Default. Modified
51. Contractor-Owned Intellectual Property. Added
52. License to Contractor-Owned Intellectual Property. Added
53. Additional Terms and Conditions. Added

51. Contractor-Owned Intellectual Property. Notwithstanding anything to the contrary in this Contract, Contractor's Software-as-a-Service (the "Software Service") solutions provided under this contract are the exclusive intellectual property of the Contractor and/or its Affiliates. All intellectual property, materials, information, documents, reports whether finished, unfinished, or drafted, developed, prepared or completed by Contractor that is related to the Software Services, including, but not limited to Contractor's Customer Data Billing solution, Engagement Builder, MyCivic, Application Builder, Meeting Manager, Content Manager, teleGov, MicroServices Platform, and derivative works or plug-ins of any of the foregoing. The Contractor's rights in this Section shall survive the termination of the Agreement. The Contractor-Owned Intellectual Property will be provided using Contractor's proprietary software, APIs, processes, user interfaces, know-how, techniques, designs, ideas, concepts, manuals and other tangible or intangible materials or information ("Contractor Technology"). As between the parties, Contractor alone (and its licensors, where applicable) own all right, title, and interest, in and to the Software Service, and Contractor Technology, or any suggestions, ideas, enhancement requests,

feedback, recommendations or other information provided by State or any other party relating to the Software Service. State will not copy, distribute, reproduce, or use any of the foregoing except as expressly permitted under the Contract. All rights in the Contractor Technology not expressly granted to the State are reserved by Contractor and its licensors.

52. License to Contractor-Owned Intellectual Property. In exchange for the State's agreement to pay Contractor in accordance with the term of this Contract and any applicable Statement of Work and rates set forth in Attachment D, Contractor agrees to provide the State with a limited, non-exclusive license for the Term of this Contract to use and receive the benefit of the Software Service in connection with the Contractor providing the services called for in the Contract and applicable statements of work.

The State is solely responsible for (i) providing and maintaining the hardware and software necessary to remotely access and use the Software Service; (ii) using frequently updated, industry standard virus and malware protection software to prevent the introduction of viruses and other malware into the Software Service from the State's network or hardware; (iii) identifying and preventing any unauthorized access to, use of, or disclosure of the Software Service or any content on the Software Service by advising Contractor promptly, but in no event more than two business days after the State learns of such access, use or disclosure.

The State shall not (and shall not permit others to) (i) modify or interfere with the Software Service or the Contractor Technology; (ii) reverse engineer, decompile, or attempt to discover the source code of the Software Service, or the Contractor Technology; or (iii) resell or otherwise use the Software Service for any purpose other than its own internal business purposes.

Contractor acknowledges that as between the parties, the State controls the means and uses of data put into the Software Service by the State or an end user ("State Data"); provided, however, that the State grants Contractor the right to use any and all State Data: (i) to perform its obligations described in the Contract, (ii) for back-up or testing purposes, and (iii) to the extent permitted by applicable law, in blinded, de-identified or aggregated form for the purpose of data analysis, compilation, interpretation, study, reporting, publishing, improvement of the Software Service, and product and service development.

State is responsible for maintaining the security of all access credentials granted to it, for the security of its information systems used to access the Software Service, and for its end users' use of the Software Service. State is responsible for all activities conducted under its login credentials. Contractor has the right at any time to terminate or suspend access to any user if Contractor reasonably believes that such termination or suspension is necessary to preserve the security, integrity, or accessibility of the Software Service, any State Data, Contractor, or Contractor's other customers.

53. Additional Terms and Conditions. Should the State choose to use any of the optional products and services the appliable product terms and conditions can be found at https://www.tylertech.com/client-terms. In the event of a conflict between any term or provision in the product terms and conditions and any term or provision in the Contract, the terms of this Contract shall govern.

Non-Collusion and Acceptance

The undersigned attests, subject to the penalties for perjury, that the undersigned is the Contractor, or that the undersigned is the properly authorized representative, agent, member or officer of the Contractor. Further, to the undersigned's knowledge, neither the undersigned nor any other member, employee, representative, agent or officer of the Contractor, directly or indirectly, has entered into or been offered any sum of money or other consideration for the execution of this Contract other than that which appears upon the face hereof**. Furthermore, if the undersigned has knowledge that a state officer, employee, or special state appointee, as those terms are defined in IC § 4-2-6-1, has a financial interest in the Contract, the Contractor attests to compliance with the disclosure requirements in IC § 4-2-6-10.5.**

Agreement to Use Electronic Signatures

I agree, and it is my intent, to sign this Contract by accessing State of Indiana Supplier Portal using the secure password assigned to me and by electronically submitting this Contract to the State of Indiana. I understand that my signing and submitting this Contract in this fashion is the legal equivalent of having placed my handwritten signature on the submitted Contract and this affirmation. I understand and agree that by electronically signing and submitting this Contract in this fashion I am affirming to the truth of the information contained therein. I understand that this Contract will not become binding on the State until it has been approved by the Department of Administration, the State Budget Agency, and the Office of the Attorney General, which approvals will be posted on the Active Contracts Database: https://secure.in.gov/apps/idoa/contractsearch/

In Witness Whereof, the Contractor and the State have, through their duly authorized representatives, entered into this Contract. The parties, having read and understood the foregoing terms of this Contract, do by their respective signatures dated below agree to the terms thereof.

INDIANA INTERACTIVE LLC

By: DocuSigned by: Andrew Hoff 281858ADDCBD413...

Title: President

Date: 5/8/2024 | 16:13 CDT

Indiana Office of Technology

By: DocuSigned by: Tracy E Barnes - 00067 05A12D6200084A8...

Title: Chief Information Officer

Date: 5/17/2024 | 13:21 EDT

Electronically Approved by: Indiana Office of Technology By: (for) Tracy Barnes, Chief Information Officer	Electronically Approved by: Department of Administration By: (for) Rebecca Holw erda, Commissioner
Electronically Approved by: State Budget Agency By: (for) Zachary Q. Jackson, Director	Electronically Approved as to Form and Legality: Office of the Attorney General By: (for) Theodore E. Rokita, Attorney General

Exhibit 1

Contract # 79743
RFP #23-74658
IOT Web Portal- IN.gov
Exhibit 1 - Scope of Work

1.0 Definitions and Abbreviations

Baseline Services	Services performed by the Contractor as part of the negotiated fixed fee portion of the contract.
CO	Change Order
Core Website	The central website of the web portal (http://www.in.gov)
Domain	Website Name
Downtime	Unavailability to the system based on third party tools
Escalation List	A list maintained by the Contractor which will set escalation paths for handling issues
FTE	Full Time Equivalent - The State defines FTE as a measurement of an employee's productivity on a specific project or contract. One (1) FTE equals one (1) legal resident or citizen of the United States fully engaged in the execution of activities or services germane to the scope of work included in this solicitation and the resulting contract; forty (40) hours a week, fifty-two (52) weeks a year.
Future Work	The design, development, testing and deployment of new applications, including legacy applications, capabilities, or significant application or capabilities enhancements that are not included within Baseline Services. These services are initiated with a Task Order (TO) and performed on a Time and Materials (T&M) basis.
“Hot” backup capabilities	A fully functional backup site with important data already incorporated, allowing for fast deployment in the case that a disaster recovery is necessary
IN.gov	The portal for most Indiana online government services
Key Personnel	Employees with key responsibilities as set by the Contractor in their Organization Chart and Staffing Plan. Key Personnel shall be located in a single office environment within one mile of the Government Center in downtown Indianapolis, IN.
Non-Disclosure Agreements	A legally binding contract establishing confidentiality

Other Governmental Body	An agency, a board, a branch, a bureau, a commission, a council, a department, an institution, an office, or another establishment of any of the following: 1. A political subdivision 2. A state educational institution
Political Subdivision	As defined in IC 36-1-2-13, any municipal corporation or special taxing district (including school corporations, municipal corporations, legislative body, taxing district, town, township, and unit).
Program	Refers to all aspects of managing and developing the IN.gov portal
Services	Work to be performed as specified in this RFP
SOW	Statement of Work document prepared for every new application, or enhancement to an existing application, to be developed by the Contractor within the Baseline Services offering
State Agency	“State agency” as used in this contract means an authority, board, branch, commission, committee, department, division, or other instrumentality of the executive, including the administrative, judicial, and legislative departments of State government
State Entity User	Any State Agency, Other Governmental Body, and Bodies Corporate and Politic that have access to and elects to use the contract
Subcontractor	Companies and/or employees employed by the Contractor to provide goods or services for the contract.
Task Order	A form used to document project requests that fall under Future Work Services
Third-Party Applications	Applications developed by someone other than the Contractor or its subcontractors or affiliates
Third-Party Portal Managed Applications	Applications developed by someone other than the Contractor or its subcontractors or affiliates which are managed by the Contractor as part of the Web Portal program
Third-Party State Entity User Managed Applications	Applications developed by someone other than the Contractor or its subcontractors or affiliates which are managed by a State Entity User as part of their online services
T&M	Work billed on a Time and Materials basis, also referred to as Future Work
TO	Task Order, a document prepared for project requests that fall under Future Work Services

	and contractor services falling outside Baseline Services
"Warm" backup capabilities	A backup site configured with storage and servers, but which may need data imported before it can be deployed for disaster recovery

1.1 Contractor Obligations and Staffing Requirements

1.1.1 Account Management and Staffing

The Contractor's staff shall be sufficient to perform the Baseline Services outlined in this Contract. This staff, the Account Management Team, shall be comprised of full-time equivalent (FTE) persons, all of whom must be legal residents or citizens of the United States.

The Account Management team shall consist, at a minimum, of Key Personnel and Baseline Service staff positions with subject matter expertise in the following areas:

- Executive Leadership
- Application Infrastructure
- Application Architecture Development
- Web Design
- Project Management
- Systems Administration
- Organization Readiness
- Security
- Quality Assurance / Accessibility
- Customer Service
- Help Desk Support and Issue Resolution
- Accounting
- Privacy
- Legal
- Human Resources
- Marketing
- Customer Experience Team

The Contractor shall be responsible for complying with all recommendations, protocols, recordkeeping requirements and best practices called for by such persons. The employees of the Contractor and subcontractors engaged by the Contractor shall be available to IOT at all times to respond to both routine and emergency situations encountered by the Contractor, and shall be made available to consult with and meet with the State as reasonably requested.

Contractor and any Subcontractors must execute all projects in the US. No offshore resources shall be allowed to work on any IN.gov or State Entity User project. Third-party resources shall be approved at the discretion of IOT prior to engagement.

1.1.1.1 Staffing

1.1.1.1.1 Organization Chart

Contractor must provide, on an annual cadence, a current organization chart identifying all Baseline Employees, contract resources and their start dates, and each person's responsibilities and make available to IOT upon request.

1.1.1.1.2 Staffing Plan

In the event that one or more essential resources become unavailable, Contractor shall provide the necessary resources to ensure timely achievement of project requirements. Contractor shall also be responsible for the identification and thorough evaluation of potential long-term resources as the situation demands.

1.1.1.2 Subcontractors

The Contractor may not use the experience or qualifications of a subcontractor to meet any of the Minimum Requirements for Responsiveness outlined in Contract Exhibit 13- RFP & Response Suite of Documents. These must be fulfilled exclusively through the qualifications and experience of the Contractor

If the Contractor seeks to meet any of the other qualifications and experience through a subcontractor, the Contractor must identify the subcontractor by name in the appropriate part of the organization chart.

The Contractor shall assume responsibility for all subcontractors.

1.1.1.3 Third-Party Vendors

The Contractor must share all contracts they have with third-party vendors that support any aspect of the IN.gov Program along with any changes that could impact the Contractor's agreement with the State.

1.1.1.4 Background Checks

As a condition of employment and for purposes of determining a person's qualifications for employment, the Contractor shall, at their own expense: undertake a criminal history record background check for all Contractor and subcontractor personnel assigned to work on the contract. Starting from day one of the contract and continuing until the contract is no longer in effect, all employees must have undergone a fingerprint based criminal history check within 60 days of being assigned to this account. The Contractor shall notify IOT in the event a background check results in a conviction finding. IOT shall determine if the Contractor employee shall be removed from the assignment.

The criminal background check shall encompass the following areas:

1. Convictions of any State or Federal crimes shall be considered if they are deemed to demonstrate a nexus to the work duties assigned to the Contractor staff Referenced under: IC 10-13-3-33.5; IC 4-13-2-14.7; IC 4-15-22-10; IC 4-15-22-30; IC 12-24-3-2; IC 22-5-1.7; IRS Pub. 1075; HEA1079-2017; Arrests & Convictions Policy
2. Exclusions by the US Office of Inspector General
3. The Contractor shall be required to retain the results of an individual's criminal history background check as long as that person is assigned to the Contract. If a currently assigned i1ndividual is promoted to a role having increased responsibility, the Contractor shall, at its own expense, perform a new background check. The results of the criminal history background check shall be made available to IOT upon request. If a conviction has been found in the subsequent background check to be related to the new role of increased responsibility, then the Contractor shall notify IOT. IOT shall determine if the Contractor employee shall be removed from the assignment.
4. If the Contractor has had a State Police fingerprint based criminal history check performed for the employee that meets the exact criteria specified above, the check may

be accepted by IOT at the State's sole discretion. Any such reference checks must have been done within six months of the contract start date.

Contractor shall require that its employees are responsible for reporting to their supervisor any arrests or convictions within five (5) calendar days from the date of the arrest or conviction. Contractor shall ensure the enforcement and administration of this provision and shall notify the State, via State Account Representative within two (2) business days of being made aware of such arrest(s) and/or conviction(s).

1.1.1.5 Confidentiality and Non-Disclosure Agreements

The Contractor shall obtain from its employees, subcontractors, independent contractors executed non-disclosure agreements. The Contractor shall require its employees, subcontractors and independent contractors to comply with any privacy or confidentiality requirements specified in an agreed-upon Statement of Work, Task Order or Change Order prior to beginning work on the particular project.

1.1.1.6 Evergreen Personnel Considerations

In an effort to foster a mutually supportive and collaborative environment in which the services are provided in an effective manner that drives value to the State, the Contractor and IOT will jointly review the performance of certain Key Personnel and Baseline Services positions, including the Contractor Account Representative.

1.1.1.6.1 Staffing Replacements and Substitutions

The Contractor must provide, on an annual cadence, a current organizational chart and staffing plan identifying all Baseline Services staff, contract resources and their start dates, and each person's responsibilities and make available to IOT upon request. The Contractor shall provide the State with a copy of the resume of each new Baseline Services employee at the time it makes an offer of employment, and shall personally introduce each new Baseline Services employee to IOT's representatives at the regularly scheduled meeting following the date the employee starts work for the Contractor. Any substitution to the organizational chart shall be announced to IOT within a week of the change.

The Contractor shall execute its responsibilities by following and applying the technical requirements, guidelines and standards in all cases in a professional and timely manner. If the State becomes reasonably dissatisfied with the work product of or the working relationship with those individuals assigned to work on the IN.gov Web Portal, the State may request in writing the replacement or reassignment of any or all such individuals and the Contractor must either replace or reassign such individual.

1.1.2 Program Management and Governance

The Contractor shall establish, utilize and monitor a governance model. This governance model shall include:

1. General Oversight of the program, including Administration and invoicing for services performed
2. Governance (advice, counsel, and feedback to IOT and the IN.gov Web Portal to enhance planning, proposal development, and decision-making)
3. Oversight of adherence to contractual requirements
4. Decisions related to data ownership, financial oversight and reporting of Contractor services, and general management and decisions that cross program areas and/or impact multiple State Entity Users.

5. Implementation of a governance structure to drive process improvements and consistency across the State
6. Conduct compliance related certifications and annual audits
7. Provide program level communications and reporting
8. Monitor and Manage Service Level Agreement (SLA)
9. Production and maintenance of development, design, architecture, security, and privacy standards
10. Reporting including a quarterly best practices report comparing IN.gov functionality with other states

Success with the IN.gov Governance Model rests largely on the effective management of operational processes that are the responsibility of the Contractor to establish and operate in conjunction with IOT and the State Entity Users. It is expected that nearly all issues are resolved through direct interaction between the Contractor and State Entity Users with IOT executive leadership participation only for escalated issues as appropriate.

1.1.2.1.1 Key Governance Staff Roles

1.1.2.1.1.1 Contractor Account Representative

During the Contract, the Contractor must designate an individual who will be primarily dedicated to the State account (the “Contractor Account Representative”) who (i) will be the primary contact for the State in dealing with the Contractor, (ii) will have overall responsibility for managing and coordinating the delivery of the services, (iii) must meet regularly with the State Account Representatives and (iv) must have the authority to make decisions and commit the Contractor’s firm with respect to actions to be taken by the Contractor in the ordinary course of day-to-day management of the Contractor’s account in accordance with this Contract.

1.1.2.1.1.2 State Account Representative

During the Term of the Contract, the State shall designate a senior level individual (the “State Account Representative”) and suitable alternates to perform this role in the event of vacation or absence who (i) shall be the primary contact for the Contractor in dealing with the State under this Contract, (ii) shall have overall responsibility for managing and coordinating the receipt of the services, (iii) shall meet regularly with the Contractor Account Representative and (iv) shall have the authority to make decisions with respect to actions to be taken by the State in the ordinary course of day-to-day management of this Contract. This Role shall provide the overall leadership and coordination for strategic governance of IN.gov services including:

1. Define the strategic business direction of Services
2. Resolve business critical issues escalated from IOT State Entity Users
3. Monitor implications of results for business performance
4. Ensure strategic goals are achieved
5. Approve changes to governance decision-making framework for services
6. Approve the addition or deletion of services
7. Approve changes to the service delivery model
8. Monitor service delivery and performance
9. Resolve issues with broad enterprise financial implications
10. Approve critical security or technology-related decisions
11. Consult on analysis of Customer satisfaction survey results and action plans
12. Review and approve changes to Service Levels, services, and performance reporting to align with business requirements

1.1.2.2 Performance Management and Issue Escalation

The governance model strives to resolve issues at the operational level. However, not all issues will be resolved at this level. The governance model shall include a mutually agreed upon escalation process designed to route the issue promptly and efficiently to the appropriate party for resolution.

1.1.2.2.1 Issue Resolution and Escalation Procedure

The Contractor shall provide an issue resolution and escalation procedure that includes the following requirements:

1. Escalation matrix with escalation contact points
2. Escalation paths for different escalation areas and levels (Critical, Urgent, Medium, Query)
3. Impact assessment which explains the level of the issue (e.g. Statewide, multiple State entities, or only a single State entity)
4. Initial response time frames and resolution time periods
5. A tracking system that assigns unique tracking IDs to each reported issue which will be maintained for the life of the contract.
6. Monthly reporting of issue resolution status to the State contract administrator and to the State Entity(s) impacted

See Contract Exhibit 11- Issue Priority Level Matrix for priority levels and corresponding plans, points of contact and timelines

1.1.2.3 Governance Meetings

The Contractor shall conduct regularly scheduled operational meetings focused on service delivery, projects, project planning, services and planning, operational status, finance, or other topics. The meeting cadence shall be dictated by IOT and shall include at a minimum:

1. A bi-weekly meeting among the State Account Representative, the Contractor Account Representative and any other appropriate operational personnel to discuss daily performance and planned or anticipated activities that may adversely affect performance or any contract changes.
2. A quarterly strategic executive meeting to ensure the visions of the Contractor and State are aligned.
3. An annual Account Representative and staff meeting to review previous year performance and plan for subsequent years.
4. A monthly meeting with IOT executives to review the status of the implementation and transition period activities.

Meetings shall include the following topics:

1. Open and honest bi-directional feedback as to overall Service performance
2. Contractor/State working relationships
3. Contractor personnel matters
4. Replacement or augmentation of Contractor Staff
5. Contractor support (or lack thereof) of State initiatives
6. Opportunities for refinement or enhancement of services or service quality and other matters as appropriate

For each such meeting, upon the State request, the Contractor must prepare and distribute an agenda, which shall incorporate the topics designated by the State. The Contractor must distribute such agenda in advance of each meeting so that the meeting participants may

prepare for the meeting. In addition, the Contractor must record and promptly distribute minutes for every meeting for review and approval by the State.

The Contractor must notify IOT's IN.gov Web Portal management team in advance of scheduled meetings with stakeholders or designated alternates (other than meetings pertaining to the provision of specific services on a day-to-day basis) and must invite IOT's IN.gov Web Portal management team to attend such meetings or to designate a representative to do so.

1.1.2.3.1 Security Governance Meetings

The Contractor shall conduct operational meetings focused on security policy, security governance, and other topics relating to the security of the IN.gov Web Portal with the IOT Chief Information Security Officer or a designee. The meeting cadence shall be quarterly at a minimum.

Meetings shall include the following topics:

1. Open and honest bi-directional feedback as to overall security performance
2. Contractor security personnel matters
3. Replacement or augmentation of Contractor security staff
4. Contractor support (or lack thereof) of State security initiatives
5. Opportunities for refinement or enhancement of security services and other security matters as appropriate

For each such meeting, upon the State request, the Contractor must prepare and distribute an agenda, which shall incorporate the topics designated by the State. The Contractor must distribute such agenda in advance of each meeting so that the meeting participants may prepare for the meeting. In addition, the Contractor must record and promptly distribute minutes for every meeting for review and approval by the State

1.1.2.4 State Entity User Technology Needs Assessment and Support

The Contractor shall meet with current and prospective State Entity Users supported by the IN.gov Web Portal as deemed necessary in its good faith and reasonable discretion, and shall discuss findings with IOT at the regularly scheduled update meetings including:

1. Review Contractor services and identify any issues or problems
2. Market and promote the benefits and use of IN.gov portal services
3. Assess State Entity User needs as they relate to their core business and related services provided through IN.gov
4. Discuss current and future projects recommended to meet their business needs*
5. Assess the existing services provided by the Contractor to see if there are any issues or needs for a technology refresh

The goal of these meetings is to determine how the Contractor, and ultimately IN.gov Web Portal, can better serve the State Entity Users and their needs. An IOT representative must be included in the Contractor's meetings with current and prospective State Entity Users.

*These recommendations could include products or services offered by third-parties, Contractor, or its affiliates and some of these recommendations may extend outside Baseline Services and may be subject to additional costs. Final recommendations subject to additional costs will be outlined in a Task Order and agreed to by all parties, including the Contractor, the State Agency, and IOT.

1.1.3 Pricing Structure

The State desires an all-inclusive pricing structure for all hardware, software, and personnel services required to maintain all IN.gov Web Portal services, applications and environments known here forward as Baseline Services. The Contractor's services delivered under this structure are to be resilient, secure, and meet the Service Level Agreements outlined in Exhibit 3- Service Level Agreements.

1.1.3.1 Organization of Service Areas

In general, there are four areas under which the Contractor services are delivered, which are outlined below:

1. **Baseline Services**: Services and operations designed to support the ongoing operations of the Contractor provided/managed computing environments and solutions inclusive of all minor and major upgrades, third party applications, personnel, and inclusive of any third-party supplies and services. Legacy applications are not included within the scope of Baseline Services for this Contract. At IOT's sole discretion, the Contractor may be engaged to develop, modify, enhance, rewrite, and replace legacy and custom applications.

   Hosting of third-party applications (those applications developed by someone other than the Contractor or its subcontractors or Affiliates) on the IN.gov Infrastructure for all Third-Party Portal Managed Applications and IOT third-party hosting requirements shall be included as part of Baseline Services. All other State Entity Users shall be given the option of Contractor hosting or IOT hosting for their Third-Party State Entity Managed Applications at the discretion of IOT after consulting with individual State Entity Users. In the event a State Entity User elects Contractor hosting, the Contractor shall bill the State Entity User directly using a Task Order and the contracted pricing in Exhibit 2- Pricing of this Contract. Exhibit 13- RFP & Response Suite of Documents includes a Current Third-Party Hosting Requirements with a listing of Baseline inclusion or State Entity User paid hosting requirements.

   As part of Baseline Services, the Contractor shall maintain all current State Entity User websites. Exhibit 13- RFP & Response Suite of Documents includes a Current Website List and a Political Subdivision Website List detailing all current State Entity Users and listings of potential State Entity Users. As part of Baseline Services, the Contractor shall add up to 200 new Political Subdivision websites annually. Contractor shall not limit the addition of non-current State Agency websites included in Baseline Services.

   As part of Baseline Services, the Contractor shall provide the following Third-Party Portal Managed Applications to all State Entity Users if required.
   - Calendar & Events Registration
   - Accessibility and Quality Assurance
   - Accessibility Screen Reader
   - Automated Web Accessibility Tool
   - URL Shortener
   - Content Management System
   - Website Search Tool

- Website Analytics
- Mapping Development Tool for Web Development (Note: The State's GIS tool will be the primary tool used for mapping)
- FAQ Solution
- Form and Workflow Builder and Management Solution
- Subscription Service for Website Stickers and Icons
- Application Style Guide
- Standard Application Header

Any updates or changes to this list of Third-Party Portal Managed Applications must be reviewed and approved at the sole discretion of IOT. An approved change will be included in an amendment to the contract.

As part of Baseline Services, the Contractor shall provide the following Third-Party Portal Managed Applications to all State Agency users if required. Political Subdivisions shall have the ability to access these at their own expense.

- Chat Bot and Live Chat Solution
- User Testing
- Web-based Org Chart Solution
- Mobile Application Solutions
- Additional Accessibility and WCAG Compliance Services

Where applicable, Baseline Service work shall be documented using a Statement of Work (SOW).

a. Baseline Services shall also incorporate a mutually agreed upon level of the following IN.gov Web Portal support elements. Any unused quantities shall carry forward into the following fiscal year. All quantities shall be utilized prior to contract close. In the event quantities are unable to be utilized, IOT and the Contractor shall determine a mutually agreed upon refund for all remaining quantities. Web Portal Support Elements includes the following:
   i. The addition of 1 new Third-Party Portal Managed Applications not to exceed an annual cost of $50,000.
   ii. The addition of 200 domain names up to $30.00/ domain/year not to include:
      1. Premium domains
      2. Domains owned by private entities

2. **Continuous Improvement Hours**: Minor alterations and enhancements (inclusive of analysis, design, construction, testing and implementation tasks) to infrastructure and application elements within the scope of the Baseline Services. The State may also request hourly consultative expertise services pertaining to business, functional or technical expertise from the Contractor. This Contract includes an annual pool of six thousand (6,000) hours. Any unused hours will carry forward into the following fiscal year.

3. **Future Work:** The design, development, testing and deployment of new applications, including legacy applications, capabilities, or significant application or capabilities

enhancements that are not included within Baseline Services. The State expects that most work conducted as part of this Contract will be performed as part of Baseline Services. State Entity Users may request additional work to be performed under this Contract via a Time and Materials Task Order to fulfill in-scope requirements not offered via Baseline Services. The rate card, found in Exhibit 2- Pricing, will be utilized for all future work. Future work shall be mutually agreed upon by IOT and the Contractor and shall be documented using a Time and Materials Task Order (TO). The Contractor may not propose rates in any Time and Materials Task Order that differ from this rate card.

4. **Political Subdivision Inclusions (Refer to Exhibit 2- Pricing for definition):** Services are to be provided to Political Subdivisions within the following classifications:
   a. Baseline Services: The following services shall be provided to any current or future Political Subdivisions as part of the fixed annual Baseline Services fee:
      - Website development and hosting on the State standard templates
        - 4 support requests per customer/month
        - Online CMS training
        - Online Third-Party Portal Managed Application training
        - 10 CMS user licenses
        - 100 migrated/built pages
        - 4 Web based forms (excluding significantly customized workflows)
      - As part of Baseline Services, the Contractor shall provide the following Third-Party Portal Managed Applications to Political Subdivision users:
        - Calendar & Events Registration
        - Accessibility and Quality Assurance
        - Accessibility Screen Reader
        - Automated Web Accessibility Tool
        - URL Shortener
        - Content Management System
        - Website Search Tool
        - Website Analytics
        - FAQ Solution
        - Subscription Service for Website Stickers and Icons
        - Application Style Guide
        - Standard Application Header

      - The Contractor must market and promote the benefits and use of IN.gov portal services

   b. Additional Political Subdivision Services: The following services shall be extended to Political Subdivisions at mutually agreed upon prices:
      - Application Development
      - Marketing and Graphics
      - Online/ web form design and access
      - Mapping Services (Note: The State's GIS tool will be the primary tool used for mapping)
      - Upgraded support, including additional support tickets, migrated pages, forms, and customized training

- Additional Accessibility and WCAG Compliance Services
- Custom Web Portal consultation
- Third-Party Portal Managed Applications:
  - Chat Bot and Live Chat Solution
  - User Testing
  - Web-based Org Chart Solution
  - Mobile Application Solutions

1.2 Infrastructure

1.2.1 Required Operating Environment & Infrastructure Technology

Infrastructure Technology refers to the composite hardware, software, network resources and services required for the existence, operation and management of an enterprise IT environment. This environment is currently designed to host and maintain for State Agency and Political Subdivision websites:

- All IN.gov supported applications
- Non-IN.gov supported, PCI compliant applications that interface with the Payment Processing Solution (Payment Processing services are provided under separate QPA Contracts and are not included in the scope of this solicitation unless expressly noted)
- All IN.gov web content
- All IN.gov supported Portal Services Software (third-party software as described in Section 1.15-Third- Party Applications)

As part of Baseline Services, the Contractor must provide any hardware and software needed to provide a separate development, test, quality assurance and production environment for the IN.gov Web Portal.

Contractor proposes to continue operating in the tier 3 hardened data centers with 24x7x365 on-site engineer support.

If at a future point in time, a transition to a cloud hosted environment is determined to be beneficial to the State and the Contractor elects to use hyper-scalers, the Contractor must utilize the State's tenant. If the Contractor elects to host in the cloud, they must choose which of the State's cloud tenants they will utilize between Microsoft Azure, Amazon Web Services (AWS), and Google Cloud Platform (GCP). The Contractor must manage their cloud environment within a carved-out space in the State tenant. The State shall bill the Contractor for their usage of the State's tenant.

1.2.1.1 Infrastructure Technology Enterprise Architecture Requirements

The Contractor shall comply with all IOT standards, policies and guidelines, which are online at https://www.in.gov/information-security-framework/. The Contractor specifically agrees that all hardware, software and services provided to or purchased by the State shall be compatible with the principles and goals contained in the electronic and information technology accessibility standards adopted under Section 508 of the Federal Rehabilitation Act of 1973 (29 U.S.C. 794d) and Ind. Code§ 4-13.1-3. Any deviation from these architecture requirements must be approved in writing by IOT in advance.

1.2.1.2 Internet Connectivity and Bandwidth

1.2.1.2.1 Internet Connectivity

The internet connectivity between the Data Center and the State and the Data Center and the user shall be provided and monitored by Contractor with respect to its sufficiency to handle

IN.gov Web Portal traffic without significant degradation in IN.gov Web Portal performance. The Contractor shall be responsible for addressing and correcting any such deficiencies, including providing increased bandwidth, if necessary. Contractor shall not be responsible for issues associated with user's phone, computer, or communication device, power made available by the public utility or internet connections not maintained by Contractor.

1.2.1.2.2 Internet Bandwidth Support

Communications between the Primary Host Data Center and any Back-up Host Data Centers to the State Data Center shall utilize Virtual Private Network (VPN). Standard traffic runs between 100 and 200MB with traffic bursts during peak times of up to 20GB. Host Data Center connections to the public must support at minimum 100 MB bandwidth with the ability to burst up to 20GB. All Host Data Center gear and ports must have the ability to burst up to 20GB. These data standards are calculated as the 95th percentile based on five-minute samples.

1.2.1.3 On-Premise Hosting

1.2.1.3.1 Data Center Standards

The Contractor shall be responsible for all fees and costs associated with the hosting of the IN.gov Web Portal at a primary facility with a secondary site with “warm” backup capabilities for non-critical systems and “hot” backup capabilities for critical systems at a location in the United States that is geographically remote from the primary site in or an Azure or Amazon Infrastructure as a service (IaaS), Platform as a Service (PaaS) or Software as a Service (SaaS) environment also at a location in the United States, or a hybrid solution. The Contractor and its proposed Data Center vendor (if applicable) are responsible for all hardware, network infrastructure, security infrastructure, server infrastructure, disaster recovery infrastructure and related tools and utilities necessary to support a web portal of this size and complexity.

The following represents key facets of the typical infrastructure required:

- Web Servers: 16 virtual servers (Production), 4 virtual servers (Test). This is subject to load, with the ability to ramp up if needed.
    - Applications servers are not included in this number, which is approximately 300 and growing.
- Load Balancers: 4 physical with additional virtual capability (2 physical appliances in each data center)
- Server Management Software and Tools Licensing:
- SQL Server Databases: 1 Development, 2 Quality Assurance (QA), 4 Production in a multi data center cluster.
- Additional Database: 1 Production Cluster hosted by the Contractor. IOT shall host the Production and Test Instance for IN.gov.
- Intrusion Prevention System
- Multi-Node Web Application Firewall
- File Upload Scanning Appliance
- Security Event and Incident Management (SEIM) Logging Tool
    - At the State’s request, the parties will explore options for the SEIM to be interfaced to the State’s security logging tool
- Logging Software
- Virtual Hosts: 10 Hosts spread across two data centers
- EMC Storage: Multiple Storage Arrays split between two data centers
- Firewalls and Switches
- Internet Bandwidth supports 2Gbps and above in multiple data centers

- DDOS appliances in both data centers
- VPN connecting the primary vendor datacenter with the IOT datacenter

1.2.1.3.2 Minimum Data Center Facility Standards (Primary and Secondary)

IN.gov shall be hosted on a primary site with one back up site with "warm" back-up capabilities for non-critical systems and “hot” back-up capabilities for critical systems including websites and the content management system. These sites shall be located in no less than two (2) facilities. The Contractor shall provide the State with evidence that the Data Center either owns or has a lease on each of the facilities where hosting occurs. Key IOT or State employees shall be allowed to reasonably inspect each facility, no more frequently than once a year, and subject to the policies and procedures of the site. Arrangements at the Data Center shall be facilitated by the Contractor. Each of the facilities where IN.gov is hosted must meet the following minimum standards:

1. *Hardened Tier-3 facility* protected by multiple physical security measures, including (a) 24/7/365 on-premise security officers; (b) a facility command station; (c) continuous closed circuit video surveillance (interior and exterior); (d) security breach alarms; (f) electronic card key access; (g) with biometric device and individual personal access code; (h) secured cage and cabinet environment; and (i) measured against HITRUST CSF Control Specifications.

2. *Technical Support*, including (a) on-site building engineers monitoring all infrastructure systems (HVAC, power, fire suppression) 24x7x365; (b) redundant monitoring performed at separate network operations center; (c) immediate customer response through Remote Hands Technical Support and dedicated hotline notification; and (d) area for pre-installation and emergency maintenance activity.

3. *Fire Detection and Suppression*, including (a) Very Early Smoke Detection Apparatus (VESDA); (b) active laser air sampling system; (c) conventional smoke and heat sensors: cross-zone throughout the center on the ceiling, below the raised floor area, top of Computer Room Air Conditioning (CRAC) units, Uninterruptible Power Supply (UPS) room, etc.; (d) pre-action dry-pipe fire suppression system, or other equivalent industry standard.

4. *Air Flow and Cooling* must meet ASHRAE's "Thermal Guidelines for Data Processing Environments", or other equivalent industry standard.

5. *Power:* Minimum of N+1 Redundancy, including (a) four (4) separate UPS systems (2N redundancy); (b) replicated configuration for dual power feeds throughout facility; (c) fifteen (15) minutes of battery backup available at full load; (d) continuous monitoring of each battery bank; (e) mission critical generators with a minimum of International Organization for Standardization (ISO) rating of Emergency Standby (ESP) located either indoors or in effective outdoor enclosures, incorporating dual starter batteries, block heaters and at least 12 hours of outside fuel capacity.

6. *Continuous Upgrade Plan*, to include new technologies, improved or best practices that may develop during the term of the Contract, subject to the IN.gov Web Portal budget and other IN.gov Web Portal resources. The State shall be the beneficiary of all such upgrades as part of the Baseline Services.

1.2.1.3.3 Minimum Data Center Non-Facility Standards (Primary and Secondary)

The primary and secondary data center shall each meet the following standards at a minimum:

1. The Data Center shall have the proven capability to achieve the 99.9% uptimes required by the State.

2. *Monitoring and Back-up.* The Contractor shall provide monitoring 24x7x365 using monitoring tools required and approved by the State. The Data Center shall provide near real time back up of the IN.gov static website content and all critical applications at its secondary site with no significant degradation of performance. Monitoring tools should include:

- SEIM: a SEIM tool that correlates logs from all security appliances as well as from web applications and web servers. Custom and standard logs shall be sent to the tool in real time. Logs should be continually reviewed by the Contractor. Alarms and reports shall be generated based on this data. Alarms are to be defined via contract as determined by the State. The Contractor's SEIM tool must integrate with IOT's SEIM tool.
- File Integrity Monitoring (FIM): a FIM tool to monitor file changes as well as network traffic to and from the server. Additionally, the tool shall track user access to the servers and report this information back to the portal's SEIM tool.

3. *Distributed Denial of Service ("DDoS") Appliances.* The Contractor shall use commercially reasonable measures to manage and appropriately mitigate risks relating to DDoS attacks including but not limited to the following:

- Providing, managing and maintaining DDoS appliances in both data centers
- These services shall receive automated updates based on global threat subscriptions to support systematically blocking of IPs based on configured threat levels. The service shall provide country block lists as well as user supported block lists while supporting configuration details that can be fine-tuned for each service/domain.
- All logging shall be sent to the portal's and IOT's SEIM tool while daily, weekly, and monthly reports can be sent to executive staff.
- The Contractor shall provide the State with a report within 4 hours of identifying the issue detailing any significant DDoS activity, including how the DDoS activity was mitigated.

4. *Web Application Firewall (WAF)*

The Contractor shall utilize enterprise WAFs to block and log suspicious activity based on specific URLs and domains. The WAF configuration shall allow the portal to tune specific policies for each application or define an overall set of security rules for a domain. As an example, the WAF supports IP reputation, rate limiting, bot mitigation, and cookie and data field validation while receiving regularly scheduled security updates. The WAF protects traffic in both data centers while security logs are sent to the portal's SEIM tool.

5. Intrusions and Data Breaches- Intrusion Protection System (IPS). The Contractor shall have intrusion detection systems and intrusion prevention systems including but not limited to the following:

- IPS support in both data centers via data center grade firewalls
- The firewalls shall monitor and block traffic based on IOT approved IPS defined policies. These rules shall be routinely checked and validated as part of the Web Portal's security program. Firewall and IPS policy blocks shall be logged and sent to the Web Portal's and IOT's SEIM tool.
- Any material reduction in the capabilities of these prevention systems shall only be made when the State has indicated that such change is acceptable to the State.

- Within 12 hours, the Contractor shall provide as much detail as is available at the time about the nature of any intrusion, and shall advise the State of all actions taken to mitigate.

6. *Incidents and Outage Response and Reporting*.
(a) In the event of a Service Outage to any critical system, the Contractor shall be responsible for contacting the State of Indiana within 1 hour of knowledge of an outage. The State shall be responsible for providing accurate contact information, including email addresses and phone numbers of appropriate designated employees. The Contractor shall be responsible for delivering an initial Incident Report to the State within 24 hours of knowledge of the incident; a detailed Incident Report must be submitted to the State within three business days after the Service Outage is initially resolved.

(b) All Incident Reports shall include the following details of the incident: Incident title with brief explanation, incident type (i.e., network), Severity, Internal or External impact, SLA-relevant, detailed explanation of incident and actions taken to resolve, State Entity User notification required, date, time, duration, trouble ticket number(s), final resolution, and an action plan to prevent reoccurrence.

(c) The Contractor shall maintain a current escalation List, including all contact information, with the State.

(d) Monitoring and reporting of outages with respect to network services shall be conducted by an independent third-party service provider, reasonably acceptable to the State, using an industry-standard tool. The Contractor shall be responsible for the costs of the third-party provider's services, and the reports shall be made available to the State. Such reports shall be exempt from disclosure under Indiana's Access to Public Records Act, Ind. Code§ 5-14-3-4(a) and (b)(l0), (11) and (19).

1.2.1.4 Operating Environment Changes
In order to mitigate potential risks and minimize the impact of changes to State operations, the Contractor must comply with the following control procedures for any changes to the Contractor provided/managed environments or supporting production infrastructure:

1. Contractor must schedule its implementation of Operating Environment Changes so as not to unreasonably interrupt State business operations.
2. Contractor must make no Operating Environment Changes that would materially alter the functionality of the systems used to provide the services or materially degrade the performance beyond the established response times established by the SLAs in Exhibit 3- SLAs without first obtaining State approval. In the case of an emergency, and in keeping with then-current State security policies, the Contractor may make temporary Operating Environment Changes at any time and without State approval, to the extent such Operating Changes are necessary, in the Contractor’s judgment, (i) to maintain the continuity of the services, (ii) to correct an event or occurrence that would substantially prevent, hinder or delay the operation of State critical business functions; and (iii) to prevent damage to the Contractor’s network. The Contractor must promptly notify the State of all such temporary Operating Environment Changes. At the conclusion of the emergency, the Contractor must restore any Operating Environment Changes to the pre-emergency state, and if the change is deemed necessary for normal operation of the

system, a corresponding change request as outlined in Contract Section 1.3.6 - Change Management must be initiated for State review and approval.

3. The Contractor must review and perform a root-cause analysis of any deviation from scheduled Operating Environment Changes and failed Operating Environment Changes.
4. Prior to using any software or equipment to provide the services, Contractor must utilize State defined testing efforts including all required testing with the exception of User Acceptance or Validation testing, which shall be performed by the State to verify that the item has been properly installed, is operating substantially in conformance to its specifications, and is performing its intended functions in a reliable manner in keeping with the defined Service Levels in effect at the time of the change.
5. Contractor must submit and gain IOT approval of a detailed project plan prior to migrating systems, environments, configurations and Contractor supplied programs from development and testing environments into production environments.

1.2.1.5 Code Based System and Environment Changes

For those System Changes (updates, upgrades, patches or otherwise) to any State system or environment within the Contractor's scope of work that involve the change of code or data (whether associated with IOT), the Contractor must:

1. Establish, publish and maintain a formal release calendar in consideration of the scheduled or required changes to IOT;
2. Develop release packaging rules that includes provisions for Contractor system and performance testing, State review and approval of Contractor results, provisions for State acceptance or validation testing (depending on the nature of the change);
3. Operational procedures to backup or otherwise copy the IOT environment prior to implementing the change;
4. Change implementation roles and responsibilities prior to making the change;
5. Rollback or reversibility considerations including success/failure criterion applicable to the change; and
6. Collaborate with IOT to develop a cohesive SDLC process between the Contractor and the State.

The Contractor must implement, utilize and maintain:

1. Industry standard code management and version control tools based on the required change management suite and approved by IOT; and
2. Requirements traceability for all elements of a system change in alignment with Contract Section 1.3.6 - Change Management.

The Contractor must:

1. Ensure that all changes adhere to State security, privacy and data handling policies;
2. Employ standard test beds that are utilized and extended for purposes of fully demonstrating completeness of adherence to business, functional and technical requirements at State required quality levels;
3. Utilize Contractor provided/managed automated methods and tools for accomplishment of routine testing functions, wherever possible; and
4. If applicable, include performance testing for high volume (transaction or data) transactions at the mutual agreement of the State and Contractor in consideration of the contents of a change.

1.3 Project Management, Change Management, and Release Control

IOT uses a project management process, known as Project Success Center (PSC) Framework consisting of four phases: Initiating, Planning, Executing & Controlling, and Closing. Contractor shall be responsible for adhering to the latest version of PSC standards, detailed at the following site: https://www.in.gov/iot/psc/.

While all projects will move through the aforementioned four phases to reach completion, the number and type of activities that a project team completes during each phase is determined by the project's classification. IOT has defined four specific complexity levels, each with its own project management requirements. Based on the project's classification, the level of project management is scaled to the size and complexity of the project. This way, smaller, less complex projects require minimal or no formal project management while large, complex projects receive a more formalized project management structure and rigor.

The processes, procedures, and service levels in this Section apply to all project management undertaken by the Contractor. Where applicable, work included within the scope of baseline services shall be completed under a Statement of Work document. Work that is inclusive of requirements outside of the scope of baseline services shall be mutually agreed upon by IOT, the relevant State, and the Contractor as to whether the project shall be completed under a Time & Materials Task Order.

IOT utilizes a website, known as Webmasters.IN.gov, for the creation of project and task requests which subsequently flow into the IOT ticketing system. The Contractor shall be required, as part of their project management strategy, to access and maintain elements contained within the Webmasters.IN.gov platform. Contractor shall be required to manage all projects relating to content, applications, third-party applications, and vanity URL's.

1.3.1 Complexity Levels

The following table outlines the IOT established differentiating factors that shall be utilized to determine a projects complexity level. Complexity levels are categorized as: Basic, Low, Medium and High. Supporting details for each complexity level can be found at https://www.in.gov/iot/psc/.

Complexity Level	Project Description
Basic	These types of projects are usually driven by an immediate business need to continue operations of an existing service or feature without further enhancements. *Typical project duration: 1 day to 6 weeks* *Time to develop charter: N/A* *Size of charter:* N/A *Sample projects: Minor bug fixes, graphic updates,* content updates,
Low	These types of projects are usually driven by an immediate business need within a short timeframe and scope may involve multiple systems or State Entity Users but with a clear authority and a simple governance structure.

	Typical project duration: 3 to 6 months with 2-5 resources *Time to develop charter:* 8 to 20 hours *Size of charter:* 1 to 3 pages *Sample projects:* New site setup, new functionality added to existing system
Medium	These types of projects usually involve more than one group or State Entity User and will include changes to both systems and business processes requiring a more complex governance structure, communication plan and risk management. *Typical project duration:* 4 to 9 months with 3-10 resources *Time to develop charter:* 16 to 24 hours *Size of charter:* 5 to 10 pages *Sample projects:* Rollout of technology across multiple State Entity Users or locations, IOT support in complex enhancement or new State Entity User system (< 3-4 servers/databases)
High	These are complex projects that typically change fundamentals about the way the business area works and includes a large amount of new development/systems. They likely span organizational entities and involve multiple stakeholders, and require a complex governance structure. *Typical project duration:* > 6 months with > 5 resources *Time to develop charter:* 20 to 40 hours *Size of charter:* > 10 pages *Sample projects:* Implementation of new technology across all State Entity Users, IOT support of a large State Entity project (>$1M)

1.3.2 Documentation Requirements

The Contractor must capture or create documentation for all project work, (whether work is performed under a SOW, TO, or Change Order CO), including establishing project specifications, milestones achievement, changes to specifications, acceptance of the final as-built project, approval for deployment, and State Entity User acceptances as agreed to in the SOW, TO, or CO. The documentation will be created in coordination with and shared with the State Entity User (s) involved in the project and IOT.

The Contractor must supply to IOT online access to all written materials, SOWs, TOs, COs, meeting minutes, documents, and artifacts related to each phase of the project, including but not limited to a Risk Assessment Plan, Communication Plans, complexity assessments, and where applicable; user manuals; process and data flow diagrams and a Requirements Traceability Matrix. This documentation should be searchable by State Entity User and

document title, and shall be deemed exempt from disclosure under Ind. Code § 5-l 4-3-4(a) and (b) (10), (11) and (19).

Documentation shall follow all guidelines as outlined at https://www.in.gov/iot/psc/. Documentation shall include but not be limited to the following documentation types:

1.3.2.1 Project Charter

A Project Charter lays the foundation of the project. IOT and State Entity User signoff on the charter allows the Contractor to begin billable work on the project.

1.3.2.2 Statement of Work (SOW)

Statements of Work shall be used for project requests initiated as part of Baseline Services. A Statement of Work (SOW) must be prepared by the Contractor's project manager and approved by IOT before any non-emergency work requiring six or more weeks of work can be started. All other Baseline Services work of less than six weeks are initiated through a helpdesk ticket submitted in the State's ticketing tool or included as part of the Weekly Status Report and presented at the regularly scheduled governance meeting with IOT.

All work performed under a Statement of Work must meet the performance criteria defined in Exhibit 3- Service Level Agreements.

1.3.2.3 Task Order (TO)

A Task Order shall be used to document project requests that fall under Future Work Services as described in Section 1.1.3 - Pricing Structure. Task Orders shall be mutually agreed upon by IOT and the Contractor prior to the commencement of work.

A TO must be prepared by the Contractor's project manager for all Future Work Services and follow the appropriate approval processes as dictated by the sponsoring State Entity User and IOT and based on the source of project funding—State Entity User or the IOT. All TOs must:

- Follow the approach described in the project documentation based on the rigor defined by the project's classification
- Be tracked in a like manner as part of a project portfolio management system
- Include a Risk Assessment to identify potential risks, their impact, and the likelihood of occurrence in order to determine the level of project management and oversight required for the project
- Include a Requirements Traceability Matrix
- Contain a not-to-exceed amount for the project, with hourly rates as set forth in the Contract

All projects completed under a TO must meet the performance criteria defined in Exhibit 3- Service Level Agreements.

1.3.2.4 Change Order (CO)

A Change Order ("CO") request, must be used to document and authorize any changes to an SOW or TO and follow the change management procedures set forth in this section.

1.3.3 Standard Operating Procedure

IOT and the Contractor shall agree on a standard operating procedure (SOP) for engaging the State Entity User. IOT shall approve the SOP and any changes to it in writing before implementation. All SOPs should include the following steps:

1. Use a Project Portfolio Management system (currently MS Project Online) to capture, manage, and measure the aspects of all projects collectively and individually.
2. Complete a Project Request Form for each new application development project.
3. Create documentation necessary to establish the required elements or specifications of project performance, including specifications, milestones achievement, changes to specifications, acceptance of the final as-built project, approval for deployment, and State Entity User acceptances as agreed to in the SOW, TO, or a CO. The documentation must be created in coordination with and shared with the State Entity User(s) involved in the project, with all final documentation and any related project changes delivered to the State.
4. Provide a project schedule with dynamically-linked tasks that represents the work required to meet the requirements and deliverables of the project documented in the Project Charter.
5. Provide a communications management plan addressing the needs of all relevant State Entity Users
6. Ensure project requirements are traceable through the entire project lifecycle.
7. Create and maintain a Risk Management plan for all projects over 1000 hours.
8. Create and maintain a RACI diagram.
9. Deliver all project documentation to IOT for review prior to delivery to any State Entity User.
10. Prepare a list of all stakeholders, with definitions of the role and associated responsibilities of each.
11. When a Project Charter is initially leveraged, estimate the amount of time it takes to complete a project schedule task as effort, in hours. The actual time shall be reported back to IOT and the relevant State Entity User via a project Task Order. The project Task Order will show what actually occurred during the project lifecycle.
12. Add IOT as an optional attendee to every meeting it schedules with the State Entity User or stakeholder.
13. Keep written meeting minutes documenting every meeting with a State Entity User or other stakeholder (whether or not related to project). The minutes shall document all commitments, decisions, or changes agreed to during the meeting. The Contractor shall create such minutes even if IOT personnel are in attendance.

1.3.4 Project Initiation

All projects must be approved by IOT before the Contractor starts work. The overall planning and scheduling of application development work shall be under the direction of IOT with priority given to "one stop" customer-focused government services, cost reduction projects, State Agency- funded projects and those governed by legislative changes. IOT has the authority to determine whether a project is a Baseline Service or will be done as a Time & Materials project with the mutual written agreement of the Contractor. Urgent Requests must be addressed as part of the regularly scheduled meeting with IOT in order to establish funding guidelines and obtain approval.

1.3.4.1 Project Development Lifecycle

IOT has developed the following Project Development Lifecycle:

1. Initiation

1. Project Initiation: IOT shall approve the project request once received. Projects are requested via the Project Request Form found on the IOT project management system, WebMasters.IN.gov through the following link https://www.in.gov/iot/psc/start-a-project/. Once approved the Contractor shall review the project request form and determine whether to proceed as a project or convert it to a ticket within the WebMasters.IN.gov system. If it is determined to be a project, the Contractor shall assign a Project Manager (PM).
2. Project Scoping: The PM shall gather necessary resources to begin scoping the effort inclusive of a kickoff meeting to gather high-level requirements, key milestones, budget, and a written business case.
3. Project Charter: The Contractor shall use everything from the kickoff meeting, and any subsequent requirements gathering efforts, to estimate effort, cost range, and draft a charter. The Contractor and IOT shall mutually determine whether the project shall be included in Baseline Services or will be done as a Time & Materials project. The requesting entity shall either approve the charter, postpone, or cancel the project.

2. Discovery
    1. Project Discovery: If the charter is approved, the project team shall gather more detailed requirements from the requesting entity and associated stakeholders. A project backlog is created via User Stories and refined via feedback from the requestor.
    2. Project TO/SOW: Once the User Stories are approved by the requesting entity, a Task Order (TO) shall be created. The TO shall detail the scope of the project and include cost and project timeline information. A SOW shall be used if the project will be covered by Baseline Services, while a TO shall be used if the project will be done as a Time & Materials project and the Contractor will bill the requesting entity for time and materials. A TO or SOW can be modified utilizing the change management process outlined in Contract Section 1.3.6- Change Management in the event that significant changes to scope are required.
3. Development
    1. Project Development: Upon requesting entity approval of the initial User Stories, the development of the requestor's project request shall begin. This shall include additional User Story refinements as the product is being developed.
    2. Quality Assurance (QA) Testing: An internal quality check of the application shall be conducted inclusive of all requirements in Contract Section 1.17- Quality Assurance to ensure all aspects of the project request are functional according to the documentation and the final User Stories.
4. User Acceptance Testing
    1. User Acceptance Testing (UAT): UAT testing begins on the application when it has passed the internal QA testing plan. UAT shall be conducted by the requesting entity team using their internal testing plan. The Contractor shall provide a UAT feedback document to track and resolve all UAT findings.
    2. Load Testing (optional): The Contractor can test the application to be sure it can handle a peak load of concurrent users. Load testing shall be done per State Entity User request. The State Entity User shall include in its request peak times the website/application will be accessed along with the expected traffic. This shall ensure the application is operating efficiently at all times.
5. Application Deployment
    1. Approval to Deploy: Once all the above steps are complete, the requesting State Entity User must provide final approval to launch the application.

2. Deployment: The Contractor shall be responsible for scheduling and conducting the application deployment.

6. Warranty/Stabilization Period: For a period of no less than two weeks after deployment, any issues/bugs found within the website/application shall be resolved, at no additional cost, by the Contractor. This shall be a heightened level of support directly after go-live.
7. Support: Contractor must have a bug/issue tracking tool set that includes a robust dashboard for tracking defects, bugs and issues and communicating status. If any issues arise with the expected functionality of the website/application after the warranty period, the Contractor will continue to support the application at no cost. Support does not include enhancements or changes to the functionality of the website/application beyond the original commitment. Changes require a Change Order to be Submitted, while Enhancements shall require a new project request.

1.3.5 Project Close Out

1.3.5.1 Close Out Survey

Customer satisfaction is a critical component of the Contractor's performance. The State requires that a Customer Close-out Survey be completed as part of the Customer Satisfaction Service Levels. Acceptable Performance Levels shall be determined by an average of 90% of surveys to be no less than a "4 out of 5". The Contractor shall create a report of recommendations to increase customer satisfaction based on the survey results and present this report to IOT at a quarterly cadence.

1.3.6 Change Management

IOT uses a common change order process that includes a CO form, provides for State Entity User notification, and includes standard steps such as create, submit, review, approve or deny. The Contractor shall use documentation templates approved by IOT, and the Contractor shall follow approved processes similar to IOT project management.

1.3.6.1 Change Management Process

The process should include, at a minimum, the following steps and/or key deliverables:

1. Notification
2. Documentation
3. Review, including cost estimation, risk assessment, and project impact evaluation
4. Approval
5. Implementation Schedule
6. User Testing/Acceptance
7. Deployment
8. Standardized methods and procedures to provide efficient and prompt handling of all changes
9. Schedule development, including approval, execution and implementation of changes

1.3.6.2 Release and Deployment Control

The purpose of Release Management is to build, test and deliver specified services that will accomplish the stakeholders' requirements and deliver the intended objectives. The Contractor shall, at a minimum:

1. Work with IOT to develop and establish a Release and distribution process so that each change to services is controlled, tested, traceable, authorized, and implemented in a structured manner.
2. Conform Contractor operations to the mutually agreed upon Release policies, processes and procedures

3. Execute releases according to the approved Release Management methodology

1.3.6.2.1 Release and Deployment Control Process

The Contractor shall propose a Release and Deployment Control process that includes, at minimum, the following:

1. Assign a Single Point of Contact (SPOC) for each Release being requested
2. Complete the proper testing for all Releases into the managed environments
3. Assign individuals to participate in the Release and Deployment Management Process, and represent the IN.gov Web Portal;
4. Participate in the functions and work activities associated with Release and Deployment Management, including:
    a. Create Release plans and perform tracking and oversight functions to support the plan documenting all aspects;
    b. Coordinate the Design, Build, and Configuration of the Release;
    c. Coordinate Release acceptance activities with IOT;
    d. Develop and implement rollout plan for the Release;
    e. Develop and coordinate Release communications, preparation, and training activities;
    f. Coordinate distribution and installation of Releases; and
    g. Provide updates to IOT management regarding Release status
5. On an ongoing basis, Contractor shall verify that only authorized users are granted access to the IN.gov Web Portal Production Environments in accordance with the Information Security Framework.

1.4 Reporting

The Contractor is responsible for developing reports in accordance with this Scope of Work and at the request of a specific State Entity User. As part of the Contractor's reporting duties, the Contractor must utilize Microsoft Project Online to complete the duties outlined in the section, unless otherwise agreed to by the State. All reporting templates that the Contractor utilizes must be standard Microsoft Project Online reporting templates or templates that are otherwise agreed to by the State. The Contractor's reports shall be driven by data and include detailed, comprehensive analyses, narratives, and/or graphics (e.g., charts, graphics, and tables) where applicable.

1.4.1 Status Reports

To convey the status of projects and Contractor activities at a high-level, the Contractor must furnish the below status reports.

1.4.1.1 Project Status Report

The Contractor shall provide the State with a Project Status Report, at a monthly cadence. The report shall provide an update on all planned and active project activity, including a Project Management Report that illustrates:

1. A status update of all projects (inclusive of Baseline Services and additional services outlined in a Scope of Work or a Task Order) by application, including:
    a. Responsible State Entity User (and point of contact)
    b. Contractor's responsible employee

c. What phase the project is in
d. An Action Item list/status update
e. Brief statements highlighting issues (if any)
f. Key dates
g. Major milestones
h. A risk assignment mitigation plan
i. A coding of Green, Yellow, or Red to signify the status at a high-level of the project, including an important data point displaying how the project is trending,
j. status of individual project areas, including schedule, cost, and quality
k. For projects outside of Baselines Services only: total project hours budgeted compared to project hours delivered, arranged by major milestone

2. A list of documents awaiting signature
3. Justifications for delayed projects
4. A list of potential revenue opportunity projects
5. A creative resource planning report by project
6. A project plan for self-funded projects, including cost and project timeline information
7. An updated organization chart
8. A Gantt chart to illustrate the overall project schedule

1.4.1.2 Monthly Performance Report

Each month, the Contractor shall furnish a monthly performance report or dashboard. This report or dashboard provides an overall picture of application development projects and status, along with the applicable SLA performance, financial reporting and data sales statistics, and select Web Portal statistics. The report shall be in alignment with and/or contain all of the information that is found in the dashboard at this link: https://www.in.gov/inwp/about-us/metrics/. The Monthly Performance Report is due within the first five – seven business days after the start of the following month. This report is publicly posted on the State's website.

The Contractor shall also develop project-specific dashboards to State Entity Users that contain key metrics relating to project status, at no additional cost to the State.

1.4.2 Management Reports

1.4.2.1 Monthly Late Log Report

The Contractor shall maintain for all active projects a Late Log Report, updated weekly, with a summary of missed milestones for the week and the reasons for missed dates.

1.4.2.2 Project Staging Report

The Contractor shall furnish a project staging report that contains all small non-complex projects that take less than 6 weeks. It also contains a report of the initial engagement(s) with the State Entity User to start formalizing an initial Project Charter, Task Order or Statement of Work.

1.4.2.3 Additional Management Reports

The Contractor shall submit Web Activity Reports, to capture web site use analytics and third-party portal managed application usage, at the direction of the State.

The Contractor shall furnish a report detailing their performance against all Service Level Agreements listed in Exhibit 3- Service Level Agreements. The Service Level Agreement report shall be delivered no later than seven days after the start of the following month.

The Contractor shall develop ad hoc or custom reports at the request of the State. Deadlines for ad hoc reports shall be determined by the State according to a scale of urgency.

1. Type 1: 24 business hours turnaround time
2. Type 2: Two (2) business days turnaround time
3. Type 3: Five (5) business days turnaround time

The State and the Contractor shall together make the determination as to whether a report is a Type 1, 2, or 3 report.

1.4.3 Financial Reports

The Contractor shall be responsible for furnishing Financial Reports (including monthly invoice reports and annual audited financial report of the Contractor).

The Monthly Financial Report shall include, at a minimum, detail on subscribers, State Entity User name, service code and name of service, State Entity User net, user fees, Contractor gross revenue refunds, returns, hosting, and task order charges and shall be in the format approved by the State. The Contractor shall prepare a quarterly report of IOT gross revenue by State Entity User and by service code, which shall be a summary and compilation of those aspects of the Monthly Financial Report.

1.4.4 IN.gov Security and Privacy Reports

The Contractor must provide the following types of reports to validate adherence to all appropriate security and privacy measures and demonstrate the “health” of the IN.gov environment.

Reports include:

1. An updated asset list to be reviewed yearly with the State
2. Results of security controls and policies audit to be delivered at a frequency to be determined by the State
3. Quarterly PCI reports
4. Results of web application vulnerability scans to be delivered at a frequency to be determined by the State
5. Monthly Potential Threat Assessment and Mitigation Recommendations

1.4.5 Web Content Management Reports

The Contractor must provide or make available the following web content management logs/reports:

1. Web server requests: All requests to IN.gov Web servers, whether application software or otherwise (including errors), are logged and archived per a back-up and retention schedule created by Contractor.

2. Web application requests: Critical IN.gov application software shall generate individual archive logs of every Web request, with the exception of personal information fields such

as social security numbers, dates of birth, credit card numbers, credit card expiration dates and banking information.

These requests must be retained for a minimum of 12 months by the Contractor.
The following are typical reports used to track the operations and performance factors of the IN.gov Portal. The State may add additional reports as needed. The Contractor shall be responsible for furnishing these reports, unless otherwise specified by the State:

1. Incident Reports
2. Current Escalation lists
3. Production Problem Response
4. IN.gov Availability reports
5. Scheduled Maintenance
6. Application Reliability of Existing and New IN.gov services
7. Support Queue
8. Infrastructure performance
9. Help Desk customer call answer time data
10. Routine performance monitoring of the IN.gov Infrastructure
11. Alert notification capability for components of the IN.gov Infrastructure
12. Graphs and statistics to measure usage of the IN.gov Infrastructure
13. Load balancing with SSL acceleration for services deployed on the IN.gov Infrastructure
14. Provide State access to a content publishing system (FTP access)
15. Provide routine traffic analysis and packet logging through a network intrusion detection (e.g., Snort) for the IN.gov Infrastructure
16. Network name services for secondary DNS

1.4.6 Reporting Functionality

The Contractor's Baseline Services staff shall be responsible for creating user accounts, using the States Single Sign On solution, for State Entity Users to view the information and reports as provided by the Contractor. The Contractor shall grant authorization to the State as "users", as necessary, to facilitate "read" access to reports provided within the Contractor’s reporting software.

1.5 Service Level Agreements (SLA) Overview

Service Level Agreements for the Contract are outlined in Exhibit 3-Service Level Agreements. The Contractor shall meet or exceed all Service Level Agreements and also monitor and maintain their performance in regard to the SLAs each month, both independently and with third party verification tools. The Contractor shall furnish a report detailing their performance against all Service Level Agreements that shall be delivered no later than seven days after the start of the following month. For more information regarding SLA reporting requirements and SLA details, please see Section 1.4.2.3- Additional Management Reports of this Scope of Work and Exhibit 3- Service Level Agreements.

The details of the SLAs may be modified during the term of the Contract. An executive SLA performance review with the State is required every 6 months. SLA performance is a key input during contract renewal.

1.5.1 SLA Liquidated Damages

The Service Level Agreements will have associated liquidated damages for failure to meet the standards. Imposition of liquidated damages is discretionary. The State will discuss and give the Contractor the opportunity to respond to performance standard issues, and may waive, give the Contractor the opportunity to earn back, or reduce the liquidated damage based on circumstances of a particular performance standard failure. Liquidated damages will be capped at 10% of the total Baseline Services cost.

Projects undertaken by the Contractor that are to be completed under a Task Order or Statement of Work may be assessed for liquidated damages. The ability to assess liquidated damages will be determined on a per-project basis, and liquidated damages will be included in a SOW/TO at the sole discretion of IOT.

If assessed, the Contractor may be given the opportunity (at the State's sole discretion) to earn back the liquidated damage amount. If the State chooses to allow the Contractor to earn back the liquidated damage, the Contractor must meet the metric in the following two reporting periods in order to earn back the liquidated damage. If achieved, the Contractor must receive verification from the State and submit a claim to have the associated liquidated damage amount returned. If the Contractor does not meet the metric in the following two reporting periods, the Contractor may not earn back the liquidated damage amount.

1.6 Training

The Contractor shall be responsible for leading or assisting the State with the training activities as outlined below:

1. Provide staffing necessary to train State Entity Users in Third-Party Portal Managed Applications on an as needed basis. For Political Subdivisions this training offering within Baseline Services pricing is limited to the list outlined in Section 1.1.3.1 item 4.
2. Provide staffing necessary to train State Agency users in their application on an as-needed basis —both on demand requests for training and as part of an overall education plan in the case of newly supported tools.
    a. Training options, including one-on-one, group training, and on-line tutorials should be made available in order to best meet the needs of State Agency users. The Contractor shall provide the State with written training materials, including templates / guides of best practices and commonly-used code, that State Agency users can independently reference.
3. Conduct web content management user training for all content managers and communicators. State Agency Users receive Web Accessibility and SEO training. This enhanced offering should be available to Political Subdivision users through a Task Order.
4. Conduct an annual security training program for all content managers including documentation/training on how to use the platform in a secure manner.
5. Develop and maintain user, provider, and operations manuals
6. Perform and/or enable baseline staff to attend or participate in applicable Web Portal-related trainings.

a. Trainings may be provided by the Contractor, the Contractor's parent company or an affiliate of the Contractor's parent company or otherwise deemed appropriate by the Contractor.

The Contractor shall develop and maintain a robust Training Plan that illustrates how they will meet the above numbered requirements. The Training Plan shall also outline the Contractor's overall training strategy and techniques. The Training Plan must include: key objectives, how they will meet the requirements listed in the bullets above, training tools, roles and responsibilities, training environments, approach and methodology, training types, materials, and effectiveness.

The Contractor must provide a sufficient number of staff to successfully accomplish all of the requirements of the Training Plan and all requirements listed in the numbered bullets above. The Contractor's training group must have proven experience in the development and delivery of comprehensive training for a project of similar scope and scale.

At any time, IOT may identify new or improved tools to be included as part of the Web Portal services. In these cases, the Contractor shall be responsible for developing and delivering trainings on these tools, unless otherwise specified by the State.

Additional training requirements related to the transition of services can be found in Sections 1.18 and 1.19 of this Scope of Work.

1.7 Help Desk and Customer Support

The Contractor shall provide Tier 1 technical support for the application software and web pages developed by Contractor ("Supported Services") to State Entity users and customer support for public users, Monday through Friday from 8:00 AM to 5:00 PM Eastern time, excluding State holidays and weekends ("Help Desk Hours"). Contractor shall provide 24/7 technical support for all Tier 2 responsibilities as determined by the State.

All help desk support shall be provided by live customer service representatives available by toll-free telephone and shall be located in the United States. The Contractor must provide staffing (e.g., customer service representatives) necessary to provide customer service help desk, billing support, and technical support for all applications and services built and/or maintained by the Contractor. The Contractor must also have the ability to ramp up support during peak usage times, such as during tax season, to ensure its ability to handle any potential increase in support call volume. The Contractor maintains the ability to increase the call center staff by 20% when appropriate to meet the needs of peak usage times. The Contractor requires notice a week in advance in order to prepare additional staff to meet peak usage needs.

Help Desk Support issues, as submitted through the Webmasters website (for more information, see Section 1.3 - Project Management, Change Management and Release Control) or by phone, include but are not limited to:

1. Non-availability of static web content
2. Application non-availability

3. Response time problems

The Contractor shall also provide help desk services related to change management issues and incidences.

The Contractor shall use the State's help desk solution software for managing content changes. All content changes will be handled by priority level and every request for a content change shall be logged through the State's help desk, which will serve as the State assignment of the content change to the Contractor. Prior approval of IOT is not required to proceed with content changes. See Section 1.11.5- Content Changes for additional details.

Help Desk tickets and inquiries shall be assigned Tiers. The Contractor's Help Desk shall respond to Tier 1 inquiries. Requests for technical or customer support that are received by the Contractor personnel and which pertain to other State applications or State system issues shall be forwarded to the State for referral to the appropriate third-party vendor or State personnel.

The Contractor shall respond to Tier 2 security and privacy inquiries, or other Tier 2 inquiries as determined by the State.

1.8 Marketing

The Contractor shall serve as a marketing arm of IOT in marketing the IN.gov web design, application development, and portal services. The Contractor must proactively market and promote to State Entities the benefits and use of IN.gov Web Portal services as part of an overall State Entity User Technology Needs Assessment and Support review as outlined in Section 1.1.2.4 State Entity User Technology Needs and Support.

In addition, the Contractor shall develop a Marketing and Outreach Plan, when requested, to include the approach for outreach and marketing and approach to reaching a broader customer / user base (e.g., Political Subdivisions).

In connection with its marketing responsibilities, the Contractor shall:

1. Use the IOT-approved change management process for all platform and tools used to support marketing changes
2. Aggregate web analytics data to gain insights and provide feedback into marketing strategies
3. Actively market its development services and seek out opportunities to increase the functionality of the IN.gov Web Portal
4. Build and maintain active relationships with nationally-recognized groups, such as, organizations like the National Association of State Chief Information Officers (NASCIO), the American Association of Motor Vehicle Administrators (AAMVA), the National Association of Secretaries of State (NASS), the Center for Digital Government (CDG) and the World Wide Web Consortium (W3C)

The Contractor shall catalog their discoveries from marketing campaigns to develop potential future road maps as the IN.gov Program works to ensure it provides the services and technologies most needed by the State.

1.9 Invoicing

The Contractor shall submit an invoice to the State requesting payment of the Baseline Services on the 15th of each month. The invoice shall contain any specific detail required under a relevant Scope of Work. The invoice shall be submitted in conformance with State guidelines and requirements regarding format, manner and time of submission invoices.

The Contractor shall submit an invoice for any Time and Materials Services performed pursuant to a signed Task Order or Change Order. The invoices shall contain the specific details required under the applicable Task Order or Change Order, and shall be submitted at the interval indicated in the applicable Statement of Work, Task Order or Change Order, or, if no interval is specified, monthly at the time the invoice for Baseline Services is submitted. The invoice shall be submitted in conformance with State guidelines and requirements regarding format, manner, and time of submission invoices. The date of submission for the invoice shall be the same date each month as agreed to by the parties.

As part of the Baseline Services, the Contractor's staff shall prepare a monthly invoice for services used on IN.gov. The form of the invoice shall be approved by the State, such approval not to be unreasonably withheld, and shall be sent to the customer's billing contact either online or by mail. The Contractor shall develop and implement procedures to utilize electronic invoices, which procedures shall be approved by the State, such approval not to be unreasonably withheld. Per-transaction charges shall be in accordance with the then-current IN.gov account agreement and applicable service schedules, and shall be subject to applicable sales and use taxes, which taxes may be charged by the Contractor in addition to the agreed-to per-transaction charges. Terms of invoice, payment shall be net thirty (30) days. IOT shall be responsible for disbursement to the proper State Entity User accounts based on the reports and invoices generated by the Contractor.

The Contractor is also responsible for maintaining a database of all transactions processed for the month, by entity, and invoicing customers on a monthly basis, with electronic invoices the preferred billing method.

The Contractor shall submit a Monthly Finance Report that accompanies each monthly invoice that provides a line-item breakdown of all Contract costs. For more information regarding Monthly Finance Reports, please see Section 1.4.3 Financial Reports.

The Contractor shall work with the State to evaluate current invoicing processes and implement any appropriate process improvements as determined during the transition period.

1.9.1 Non-Electronic Payments from Users

The Contractor will provide monthly account users who do not pay electronically with a monthly invoice either online or by US mail. The Contractor will establish a lock box to receive all paper payments of monthly account invoices. The Contractor is responsible for all fees associated with lock box account maintenance and support.

All monthly account paper check payment funds must be deposited to the State-designated bank account via a lockbox. The lock box service provider is responsible for depositing the contents of the lock box in the bank designated by the State. The State uses the Account Database or System (as outlined in Section 1.16.1 Account Database) maintained by the Contractor, the Lock Box report and the corresponding Bank Deposit receipt to reconcile payments. The Contractor is not an active party to the deposit and disbursement of the funds to the State and is not responsible for the amount or for the schedule of deposits to the State from the paper check users.

1.10 Security

Security of the IN.gov Web Portal and protection of non-public information transmitted through and over the portal is of paramount importance to the State. The following terms and conditions apply to all services provided by the Contractor on behalf of the State, whether a Baseline Service or Time & Materials, and whether data is housed at the Data Center or elsewhere.

1.10.1 Background

Security is defined as “protection against unauthorized access to, or alteration of, information and system resources, including CPUs, storage devices and programs” or “the state of being free from danger or threat.” In an effort to continue to provide optimum security protection for all systems and applications that support the IN.gov Web Portal, the Contractor must provide support staff as part of Baseline Services for three critical areas:

- Security
- Privacy
- Compliance with any/all Federal, State and other laws, rules and regulations

The security and privacy staff assigned to this program area shall provide comprehensive, day-to-day operational security and privacy support for the three hundred plus (300+) websites and growing, securing infrastructure components that process over ten (10) million financial transactions annually, and the application software that is developed and maintained for the State and in production on IN.gov.

Security and Privacy includes:

- Compliance to all standards governing data security and includes data entry, storage, access, backups, and transaction logging and reporting
- Security Policy
- Privacy Policy
- Security Awareness Program
- Privacy Program
- Privacy Awareness Program
- Security Architecture
- Privacy Architecture
- Disaster Recovery/Business Recovery/Business Continuity Plans
- Management of PCI DSS requirements, PHI and Personally Identifiable Information (PII) protection requirements

1.10.2 Compliance with Established Standards

At a minimum, the Contractor shall comply with the following:

1. State's most current Information Security Framework, which is based on the National Institute of Standards and Technology standards (NIST.gov).

2. Maintain an on-going security enterprise certification based on NIST standards
3. Provide a Certificate of Cyber Insurance, annually
4. The Contractor shall comply with the State's Cloud Product and Service Standard ID: IOT- CS-SEC-010.
5. The Contractor shall, as applicable and at its sole expense, comply with the following industry standard best practices unless otherwise agreed to by the parties:
    a. The latest versions of NIST SP 800-53 and 800-53A for data in use, in transit, and at rest.
    b. The latest versions of NIST SP 800-53A, NIST SP 800-30, NIST SP 800-37, NIST SP 800-115
    c. The latest version of CSIS 20 Critical Security Controls
    d. Payment Card Industry Data Security Standard ("PCI DSS"), and shall provide an Attestation of Compliance upon request (if applicable)
    e. NACHA Operating Rules (if applicable)
    f. SOX Security Compliance
    g. Web Accessibility Initiative's (WAI) Web Content Accessibility Guidelines (WCAG) 2.0
    h. The latest version of the Indiana Office of Technology's TLS standards and requirements
    i.

1.10.3 Third Party Enterprise Agreement

The Contractor shall maintain an Enterprise Security Assessment or a similar third-party assessment, and shall annually provide the State with evidence of such assessment. When requested by the State, the Contractor shall make available risk assessments performed in conjunction with this section for review by the State. The Contractor shall select another similar third-party assessment offered by a nationally recognized firm, if available, or Contractor shall retain another third-party security company of its choice to perform a comprehensive security audit in connection with the services being performed by Contractor under this Contract. The Contractor shall remediate any deficiencies found by the third-party security assessor based upon a mutually-agreeable risk scoring standard, such as the Common Vulnerability Scoring System ("CVSS"), to ensure that changes are implemented in a timely manner for known vulnerabilities. The Contractor must keep their reports in line with SOC 2 Type 2 standards. Any risk assessments or security audits performed in connection with this Section shall be deemed exempt from disclosure under Ind. Code § 5-14-3-4(a) and (b) (10), (11) and (19).

1.10.4 Security, Risk Monitoring, and Assessments

All documents associated with the following subparagraphs shall be deemed exempt from disclosure under Ind. Code § 5-14-3-4(a) and (b)(10), (11) and (19).

1. The Contractor shall maintain a formal, defense-in-depth Security Incident Response Plan, which shall describe how the Contractor will respond to security incidents and shall also describe the security strategy that will be used to provide ongoing security for State resources in the Contractor's environment. The Security Incident Response Plan shall be updated on an ongoing basis, with updated copies provided to the State. As part of ongoing security support, the Contractor must inform the State of both offensive and defensive strategies in place in the Contractor's environment.
2. The Contractor must complete and deliver a formal security risk self-assessment of the Contractor's environment, with a strategy and action plan to address identified risks.

Updates to the assessment must be delivered to and reviewed with State security staff quarterly until all identified risks are resolved.

3. The Contractor, using its own staff or a subcontractor, shall provide an internal security auditor, who is PCI DSS certified, to consult with the State on PCI DSS and security matters in relation to the Contractor's payment processing program.
4. The Contractor shall utilize a security testing approach that aligns with NIST 800-115, Technical Guide to Information Security Testing and Assessment.
5. The Contractor shall provide continuous monitoring, based on applicable NIST 800-137 guidance, of the technical environment(s) that house State applications. The Contractor shall conduct comprehensive manual and automated reporting on a regular basis, the results of which must be provided to the State at least monthly, and on demand by the State when necessary.
6. The Contractor shall complete an appropriate PCI DSS Self-Assessment Questionnaire on an annual basis, shall conduct quarterly network vulnerability scans conducted in accordance with PCI DSS requirements, and shall annually conduct application penetration testing with a third party on applications developed by the Contractor that accept PII, PHI, or payment processing information within the application.
7. The Contractor shall continuously monitor and, to the extent it receives information specific to the State of Indiana, provide to the State real-time, up-to-the-minute threat intelligence to include strategic (through recognized national and global security sources) and tactical and operational/technical intelligence. Any changes to the threat landscape that could reasonably and materially impact the State must be communicated in writing and include advice on action to be taken by the State if required.
8. The Contractor shall employ the Intrusion Detection Systems and Intrusion Prevention Systems, which will be supported with current technology.
9. Contractor must participate in quarterly meetings with designated State security staff to provide security activity updates. These updates must be compiled in line with SOC 2 Type 2 standards.
10. Any third party engaged by the Contractor to perform security testing, monitoring, or external network vulnerability assessments shall be approved, in advance and in writing, by the State. The Contractor shall remediate any deficiencies found by any third-party security assessor based on a mutually-agreeable risk scoring standard to ensure that changes are implemented in a timely manner for known vulnerabilities. The Contractor and IOT shall meet annually before security testing commences to agree upon a risk scoring standard.

1.10.5 Disaster Recovery and Business Continuity

The Contractor shall maintain and share with the State a Disaster Recovery Plan, and shall make available to the State all amendments, changes, or modifications to its Disaster Recovery Plan, which is deemed a trade secret and is deemed information that would jeopardize a record keeping or security system, and shall be exempt from disclosure under Indiana's Access to Public Records Act, Ind. Code § 5-14-3-4(a) and (b)(10), (11) and (19). This is in addition to, but may include, the Disaster Recovery Plan required for the Data Center. The Contractor shall, in coordination with the State, maintain a specific Business Continuity Plan dedicated to operating State systems for which it is responsible in the event of a disaster.

1.10.6 Security Plan

1. The Contractor shall have in place a comprehensive Security Plan and Internal Control Plan.
2. The Contractor must provide a formal, defense-in-depth security strategy, 30 days from contract execution, that will be used to provide ongoing security for State resources in the Contractor environment, update the strategy on an ongoing basis, and inform the State in writing within thirty days of strategy updates. As part of ongoing security support, the Contractor must inform the State of both offensive and defensive strategies in place in the Contractor environment.
3. The Contractor must utilize a security testing approach that aligns with NIST 800-115, Technical Guide to Information Security Testing and Assessment.

1.10.7 Audit Controls

The Contractor shall obtain and provide a copy of the annual independent audit of the Data Center(s) at its expense and shall, upon completion, provide an un-redacted version of the complete audit report to the State. A Service Organization Control (SOC) 2 audit report or equivalent approved by IOT sets the minimum level of a third-party audit. The State may also perform an annual audit of the Contractor's collocated space within its Data Center(s). The audit may take place onsite or remotely, at the State's discretion. The State shall provide to contractor thirty (30) days' advance notice prior to the audit. The Contractor shall make reasonable efforts to facilitate the audit and shall make available to the State members of its staff during the audit. The State may contract with a third-party to conduct the audit at its discretion and at the State's expense. The audits conducted under this paragraph are deemed information that is a trade secret and that would jeopardize a record keeping or security system, and shall be exempt from disclosure under Indiana's Access to Public Records Act, Ind. Code § 5-14-3-4(a) and (b) (10), (11), and (19).

The Contractor shall provide an audit trail for all transactional and administrative tasks. The Contractor's portal support must provide the capability to maintain access roles that dictate permissions for system/application access. Roles may be added, updated, or deleted by an Administrator. The Contractor shall store log capture information for a minimum of one year from date of capture. The Contractor shall perform annual internal security audits to help thoroughly test Contractor's security posture. Audit reports and risk mitigation plans must be made available for review by the State one month after completion, and shall be deemed exempt from disclosure under Ind. Code § 5-14-3-4(a) and (b) (10), (11), and (19).

1.10.8 User Accounts

The Contractor shall adhere to applicable NIST standards and best practices governing management of user accounts, such as time-driven auto disablement, account deletion, locking of accounts, and maintenance of user profile data following deletion. User accounts shall be reviewed for inactivity at a quarterly rate at minimum and appropriate action taken; auto disablement, account deletion and/or locking. When possible, the Contractor shall use the State's SSO to manage user accounts. User accounts must follow IOT password complexity requirements. Accounts with privileged access which are authenticated by the Contractor are required to have at least NIST 800-63 AAL-2 authentication. The Contractor shall provide the capability for password encryption before the password is recorded in any data repository. Passwords shall not be stored directly; rather, a cryptographic hash of the password shall be stored. Password hashing must adhere to NIST 800-63B Section 5.1.1.2.

1.10.9 Software Security Features relating to IN.gov Infrastructure

In addition to the security requirements imposed on the Data Center above under Section 1.2.1.3.2 Minimum Data Center Facility Standards, the Contractor shall provide, at a minimum, the following software security features for the IN.gov Web Portal:

1. "Stateful" or equivalent inspection firewalls shall be used to help regulate all network traffic from the internet into the DMZ segments and communications between network tiers.
2. Infrastructure that supports a configuration that performs as a DMZ for Contractor-supported State applications.
3. A multi-tier application architecture shall be used to help limit communications between the tiers to mitigate against an intruder from accessing critical systems attached to network segments.
4. VPNs or another means of secure communication agreeable to the State shall be used to help prevent unauthorized internal intercept of communications between IN.gov and State systems.
5. Intrusion detection products shall be used to help identify and report intrusions to the Contractor's staff so they make take immediate counter-measures.
6. Virus protection software shall be used to help proactively identify computer viruses.
7. Development workstations shall be secured in a commercially reasonable manner to mitigate the risk that an intruder will gain access to the server infrastructure through a compromised workstation.
8. Remote access by portal employees shall utilize VPN client software using multi-factor authentication mechanisms to mitigate the risk of unauthorized remote entry into the system.
9. Identify security incidents which penetrate the IN.gov servers maintained by Contractor and compromise data (defined as obtaining or altering confidential user information, transaction data, or authorized static content), and shall notify the State within two (2) hours of confirmation of the incidents.
10. The Contractor shall maintain and follow a patch management Standard Operating Procedure reasonably acceptable to the State designed to provide a secure network environment for its applications, staff, business partners, and contractors so that all electronic devices (including servers, desktops) connected to IN.gov network have proper virus protection software, current virus definition libraries, and the most recent operating system and security patches installed. The Contractor shall report any exception to the Standard patching schedules to the State.

1.10.10 Protection of Personally Identifiable Information

"Personally Identifiable Information" in Ind. Code 4-1-11-3. This paragraph supplements the requirements of the Contract relating to confidentiality of State Information, PII, and the Security and Privacy of Health Information. The Contractor shall comply with the following privacy standards (and the State shall require all agencies using IN.gov, and shall require any third-party vendors providing applications to IN.gov, to comply with the same):

1. Not less than IOT's TLS encryption standards to protect Web requests that contain as applicable:
    a. User credentials (username and password)
    b. Sensitive information (credit/debit cards numbers, checking account and routing numbers) and any forms of user authentication
    c. Personal information as defined by Ind. Code § 4-1-11-3
    d. Personal information as defined by Ind. Code § 24-4.9-10

e. Highly restricted personal information in a driving record as defined by Ind. Code § 9-14-16
f. Protected health information as defined by the Health Information Technology for Economic and Clinical Health Act

2. Documenting, for each application, what information will be accessed, how it will be accessed and provided to the public, an assessment of the access method and what, if any, special authentication requirements must be satisfied by the individual customers to qualify for access. Such documents are deemed information that would jeopardize a record keeping or security system, and shall be exempt from disclosure under Indiana's Access to Public Records Act, Ind. Code § 5-14-3-4.
3. The Contractor shall ensure that all PII is housed in the continental United States, inclusive of backup data.
4. The Contractor must provide a system that shall encrypt all financial and confidential data transmissions.
5. The Contractor's protection of all data retained by Contractor from IN.gov users shall adhere to current Contractor and IOT-specified security policies in effect at the time of deployment of the application. The service shall also comply with the then-current applicable privacy policies established by the State or the applicable State Entity User, and state, and/or federal law. In the event a change to the State's or a State Entity User's privacy laws and/or security policies results in increased Contractor costs, the Contractor shall notify the State of the cost associated with compliance, and the State shall bear the increase. In connection with any services being provided to agencies under Statements of Work or Task Orders, the State Entity User must inform the Contractor promptly of relevant changes in the privacy laws and/or security policies that impact the services being provided by the Contractor.
6. Upon State request, the Contractor shall provide a copy of all PII it holds. The Contractor shall provide such data on media and in a format determined by the State.
7. Upon termination of this Contract and in consultation with the State, the Contractor shall destroy all PII it holds (including any copies such as backups) in accordance with the current version of National Institute of Standards and Technology ("NIST") Special Publication 800-88. The Contractor shall provide a written confirmation of destruction to the State within ten (10) business days after destruction.
8. All data movement within or out of the State environment must utilize an approved State provided process.

1.10.11 Privacy

In addition to the protection of Personally Identifiable Information, the Contractor shall protect the privacy of users and information as follows:

1. The Contractor shall have a written Privacy Program which reflects commercially reasonable practices for privacy programs and incorporates the use of privacy-by-design techniques, including using data de-identification tools for adequate PII and PHI protection when required. The Privacy Program shall be updated as needed by the Contractor and approved by IOT. The Privacy Program is subject to annual review by IOT. The Contractor and IOT shall work in good faith to develop a plan to address the concerns of IOT.

2. The Contractor shall designate a single point of contact (“SPOC”) for all privacy matters. The SPOC shall be familiar with HIPAA and HITECH and the Contractor shall also have a resource with a CIPP/US certification.
3. The Contractor shall have controlled user access, restricting access to all PHI and PII to those staff members with a job-related need for access.
4. The Contractor shall submit a Privacy Impact Assessment format plan annually, for approval by IOT, prior to execution of the Privacy Impact Assessments. Such assessments may use the decision tool used by U.S. Department of Homeland Security to identify and mitigate privacy risks on all re-developed and newly-developed systems and applications that house PII and shall complete a Privacy Self-Assessment for locations under the control of the Contractor that house systems and applications supporting the IN.gov portal.
5. The Contractor shall maintain a Privacy Incident Response Plan, either as a standalone document or as part of its current Security Incident Response Plan, a copy of which must be shared with the State for its review. The Plan shall be reviewed and updated annually.
6. The Contractor shall assist the State in its compliance with Ind. Code § 4-1-6 as it applies to the Contractor’s systems that collect PII. This includes, but is not limited to, data regulated by HIPPA and FTI.
7. If the Contractor handles federal tax information (“FTI” – defined in IRS Publication 1075, §1.4 [November 2021]) the Contractor must comply with applicable NIST and IRS Publication 1075 security controls and requirements to which the State subscribes. As an example, if the Contractor handles FTI for the Department of Revenue, then the Contractor must comply with all applicable aspects of the NIST 800-53 pertaining to safeguarding such data.
8. The Contractor must ensure that all data is housed in the continental United States.

1.10.12 Disclosure of a Security Breach

Ind. Code § 4-1-11 is applicable to the breach of the security of a system that houses information maintained by a State Entity User. If such a breach occurs and involves information in the possession of the Contractor, the Contractor shall fully comply with the notification and reporting requirements of that statute. The Contractor’s performance under this Contract is governed by, among other things, Ind. Code § 24-4.9. The contractor shall comply fully with Ind. Code § 24-4.9, and shall:

1. Notify IOT as soon as it discovers that there has been a breach of the security of data as defined by Ind. Code §24-4.9 (an “Incident”).
2. Notify IOT and the Indiana Attorney General to the extent required by the Ind. Code § 24.9-3-1 within two (2) hours of the confirmation of an Incident. To the extent possible, the parties will follow a mutually-developed Communications Plan and Incident Report detailing the Incidents covered and the reporting and notification requirements under Indiana statute; such reporting and notification may include information specifically identified as confidential or trade secret by the Contractor.
3. Implement and maintain procedures consistent with the requirements of this Contract, including taking commercially reasonable steps to protect and safeguard from unlawful use or disclosure of all Personal Information that is collected and maintained by the Contractor under this Contract.

4. Notify IOT, and the affected persons as required, of any Incident caused by the Contractor's breach of the requirements of this Section where unencrypted personal information was, or is reasonably suspected to have been, acquired by an unauthorized person through the Contractor's systems, or encrypted personal information was or may have been acquired through the Contractor's systems by an unauthorized person with access to the encryption key. However, the Contractor may delay providing notice to the affected persons (1) when the delay is necessary (a) to restore the integrity of the computer system or (b) necessary to discover the scope of the breach; or (2) at the request of the Indiana Attorney General or any law enforcement agency if the disclosure will (a) impede a criminal or civil investigation; or (b) jeopardize national security. The notification to the affected persons delayed under (1) shall be made as soon as the delay is no longer necessary to restore the integrity of the computer system, or to discover the scope of the breach. The notification to the affected persons delayed under (2) shall be made as soon as the Indiana Attorney General or the law enforcement agency notifies the Contractor that disclosure will no longer impede an investigation or jeopardize national security.
5. Notification to affected persons of an Incident caused by the Contractor's actions or lack of action shall be made by the Contractor at the Contractor's expense and shall comply with the notification requirements of this Contract and applicable law. Additional remedies, such as making available to the affected persons credit monitoring and call center support shall be conducted as required by law, or otherwise as mutually agreed by the parties.
6. The Contractor shall pay all final judgements, and reasonable attorney fees, and associated court costs due to an Incident that is directly attributable to the Contractor's actions or lack of action.

1.11 Websites

1.11.1 Website Staffing

The Contractor shall provide a Creative Services team that includes a dedicated Senior Creative Manager with experience using UI/UX design. The design team is responsible for website redesign projects and professional graphic design, custom HTML, JavaScript, and CSS assistance.

1.11.2 Website Design Standards

The Contractor is responsible for establishing, maintaining, and updating website design standards to promote a consistent experience across websites and applications. The Contractor is responsible for the implementation of new web sites as requested by State Entity Users in accordance with the standard IN.gov look and feel. These standards shall include at a minimum:

1. An Application Style Guide
2. A standard application header
3. A Web Design Standards and Requirements Document
4. Code reusability
5. User experience tools that are intuitive, accessible to all levels of technical expertise, and promote quick deployment of websites, applications, and standards

1.11.3 Website Design Tasks

The Contractor is responsible for the following web design tasks:

1. Content changes - which must be handled on a priority level

2. Graphical element design
3. Creation of prototype templates as part of the development process
4. Consistent application look and feel
5. Application prototyping
6. Application landing page design
7. Compliance with § 508 of the Rehabilitation Act of 1973 (Accessibility Standards) with Level A (must support) and Level AA (should support) Success Criteria as defined under Web Content Accessibility Guidelines (WCAG) 2.0, in each case with respect to public-facing portions of the systems.
8. Billboard creation
9. Web 2.0 Social Media Requests for Social Media tools including, Twitter, Facebook, YouTube, Blogging, and RSS Feeds
10. Web CMS maintenance in accordance with the current IN.gov look and feel
11. Conduct frequent user experience testing sessions on website templates and applications

The Contractor shall integrate all IN.gov web technologies in new websites and applications as part of the base design or template inclusive of any advanced features and integrations.

In connection with its web design and marketing responsibilities the Contractor shall:

1. Use the IOT-approved change management process for all platform and tools used to support web design and marketing changes
2. Monitor and process all web content-related requests logged through the IOT Webmasters solution
3. Maintain a response time of at least 200 milliseconds but no more than 1 second for all web pages and report response time on a monthly basis against this Metric
4. Aggregate web analytics data to gain insights and provide feedback into marketing strategies
5. Actively market its development services to the agencies and seek out opportunities to increase the functionality and self-service features of IN.gov
6. Provide § 508 Accessibility Compliance Reports via industry standard accessibility tools as directed by IOT

1.11.4 Procedural Requirements

Web design services shall be provided by the Contractor, including development of templates used by IN.gov customers, as a part of Baseline Services. Agencies shall make requests through the Webmasters system as a part of Baseline Services.

Agencies shall have the ability to request assistance with maintaining non-interactive portions of their web presence through an online request via the Webmasters Platform. This shall include such things as HTML, HTML5, JavaScript, CSS, CSS3, graphics, images, and simple email contact forms. The standard turnaround time for these requests shall be three business days.

1.11.5 Content Changes

All content changes will be handled by priority level. The Contractor shall use the State's help desk solution software for managing content changes. Every request for a content change shall

be logged through the State's help desk, which will serve as the State assignment of the content change to the Contractor. Prior approval of IOT is not required to proceed with content changes.

Priority levels are defined as:

- High: Requires immediate changes
- Medium: Requires changes within a 2–3-day timeframe
- Low: Work that has a due date in excess of 3 days

1.11.6 Continuity of Services

If the Contractor has a maintenance issue that causes services to be unavailable, including the IN.gov static website, the Contractor shall provide a static page that links to high profile services not hosted by the Contractor.

1.11.6.1 Back-Up Copy

The Contractor must provide an annual back-up copy of the IN.gov website to meet the State's record retention policy. The back-up must be in a format acceptable to the Indiana Archives and Records Administration (IARA).

1.11.7 Web Technology Integration and Support

Contractor shall provide, maintain, and manage services available on IN.gov that include but are not limited to:

- Assistive technology
- Online Calendar
- FAQ/Live Chat
- Web-based email subscription management system
- Mobile Application Solutions
- Content experience and marketing performance tools
- Workplace productivity tools
- Maps for websites and applications
- Search Appliance
- Stock imagery resource

As part of Baseline Services, the Contractor shall keep all IN.gov-supported and hosted, third-party, portal service applications current, shall monitor release announcements, perform software updates on a timely basis following the State's notification protocol, coordinate with IOT in defining third-party application hosting standards, and must maintain version control history and documentation for all IN.gov supported, third-party portal service applications as outlined in Section 1.15 Third-Party Applications.

1.11.8 Website Domains

As part of Baseline Services, the Contractor shall be responsible for the management of current public and internal facing websites and domains, as well as subsequent addition of websites and domains.

1.11.8.1 Vanity URL's

Contractor shall manage and maintain all vanity URLs and provide a process by which State Entities can determine the active status of each URL at renewal points. Exhibit 13- RFP & Response Suite of Documents includes a listing of current Vanity URLs.

Any State entity on the IN.gov network shall have the ability to request specialty URLs including .com, .net, .org, etc. Review and approval by IOT shall be required for all requested URL's.

In accordance with IOT policy, all vanity URL (non-IN.gov) domains are subject to a third-party domain registration fee and must be kept indefinitely once purchased. Contractor shall work with the requesting State Entity User to determine the appropriate registration period for each requested vanity URL. Contractor shall pass through the registration fee to the requesting State Entity User via a Task Order.

The Contractor shall notify IOT and the State Entity User using the vanity domain(s) 90-days before expiration to initiate the renewal process.

1.11.8.2 Refreshes

Under the direction of IOT, the Contractor shall design, plan, schedule and then execute a biennial technology refresh of the IN.gov home page, which includes applications, web services, and web integration technology that integrates with home page and are branded with the same header and footer of the IN.gov Home Page.

The Contractor shall continuously look to identify emerging technologies and standards to improve capabilities and increase performance. This research shall include user testing and focus groups. As part of biennial technology refresh, the Contractor shall present the findings of such research with recommendations to the State.

The Contractor shall be responsible for executing a refresh of the IN.gov home page and related non-State Entity pages every other year, at a minimum, and a refresh of State Entity home pages in the alternate year. State Entity websites must conform to the web design standards and layout templates as directed by IOT. The Contractor must then work with each of the agencies to adopt an appropriate template and create a fresh look for presenting State Entity content and links.

The Contractor shall keep IOT informed of new software release schedules as part of the overall technology refresh strategy.

1.12 Content Management Systems (CMS) Requirements

Enterprise Web Content Management shall encompass support of the State's Web Content Management System (WebCMS), overall web technology innovation and implementation, and responsibility for planning and executing the recurrent web technology refresh.

1.12.1 Operational Requirements

The Contractor shall provide, manage and maintain a Web Content Management System (WebCMS). This includes:

1. Maintaining the software
2. Standards as established by the Contractor and approved by the State
3. Processing requests for content changes
4. Ensuring integrity of links on the Core Website
5. Comply with § 508 for public-facing aspects under the Contractor's control
6. Conducting user training for State content managers and communicators as mutually agreed in writing
7. Partner with the State in communicating with any WebCMS vendors

The Contractor shall manage content and images purchased by it for use on the IN.gov Web Portal. Contractor must also provide a mechanism for State Entity Users to submit their content and images for management, which may be integrated into the current asset manager using a global asset manager. The State is responsible for any content submitted by a State Agency pursuant to this Section and the Contractor shall not have any liability if such content violates any third-party rights. Political Subdivisions are responsible for any content submitted by them pursuant to this Section and the Contractor shall not have any liability if such content violates any third-party rights.

All websites and applications must incorporate the State's Enterprise Web Analytics tool as part of the design. The Contractor must design web solutions to be brand-able with data driven configuration, and must provide UI (User Interface) mockups to stakeholders for new user interfaces or changes to existing user interfaces.

All web pages must use the IOT-approved web analytics software. When major design changes, as determined by the State, are made to the portal, Contractor must have an established relationship with a third party to provide analysis and focus group feedback as part of Baseline Services.

1.13 Innovations and Trends

1.13.1 General Innovation

The Contractor shall recommend innovative solutions for:

1. Improving the presentation and delivery of e-government services to users,
2. Creating revenue streams for the State government as a way to offset both the cost of technological improvements and the cost of conducting State business. As part of an innovation strategy, the Contractor must seek out and evaluate third-party web solutions to address across-State Entity User needs and present their recommendations annually.

Contractor shall meet with State Entity Users supported by IN.gov as deemed necessary and with IOT at a minimum of once a year to:

1. Market and promote the benefits of IN.gov portal services
2. Discuss current and future projects to meet the business needs of State Entity Users,
3. Assess the existing services provided by the Contractor to determine if there are issues or needs for a technology refresh
4. Discuss and provide updates to the State on industry-wide trends in the Web Portal space

If requested, the Contractor shall provide written materials informing State Entity Users and/or IOT of applicable industry trends, discuss potential innovations and improvements to the Web Portal.

1.13.2 Technology Innovation

The Contractor shall assess the current CMS solution, propose an alternative product, and if applicable, complete a proof of concept that will allow the State to determine the viability of the CMS during the performance period. The assessment will be in the form of a formal project that will detail the processes and procedures followed. The deliverables of the assessment may include the following:

1. CMS requirements as defined by the existing software and through interviews with the IN.gov Advisory Council.
2. Analysis of at least 3 leading content management system providers to determine which meet the requirements, as well as any deficiencies.
3. Review and approval of the requirements and analysis by IOT and the IN.gov Advisory Council.
4. In the event that one of the products evaluated is determined to be a viable replacement for the current CMS, and selected by IOT, after consulting with the IN.gov Advisory Council, the Contractor shall work diligently to complete a proof-of-concept using the product selected. Details of the proof-of- concept shall be defined in mutually agreed to Statement of Work.
5. Upon successful execution of the proof-of-concept, and selection by IOT, the Contractor shall work diligently to assist the State in migrating from the current CMS to the selected product according to the terms in a mutually agreed upon Statement of Work or Task Order.

1.13.3 Competitions

On a yearly basis, the Contractor is responsible for identifying relevant national and/or international competitions such as the Government Experience Awards- and submitting the IN.gov website for consideration.

1.14 Applications

The Contractor is responsible for the security and integrity of all applications it develops for deployment by the State. In addition to the requirements set forth below, all applications developed by the Contractor shall adhere to the applicable requirements set forth above in Section 1.10 - Security. These requirements apply regardless of whether an application is developed as part of the Baseline Services under a Statement of Work, or under a Time & Materials Task Order.

All services and applications, whether developed as part of Baseline Services or as a Time and Materials Task Order, must be supported and maintained by the Contractor as part of the Baseline Services fee.

The Contractor shall ensure that all data-related connections or Application Programming Interfaces (APIs) between entities utilize MuleSoft.

The Contractor must use the State’s Single Sign On Enterprise Authentication standard (SSO) for all applications requiring user sign-in.

1.14.1 Application Software

The Contractor shall conform to applicable industry practice in its application development. All applications will be developed by Contractor based on secure coding guidelines such as the Open Web Application Security Project Guidelines ("OWASP") Top 10 and the CWE/SANS Top 25 Programming Errors published regularly by the SANS Institute. Contractor must build security credentials into each newly-developed application, and shall use application scanning software and a process to promote the release of secure code at the time such code is put into production. The Contractor will use commercially reasonable efforts to implement appropriate changes required by updates published to the guidelines.

The Contractor shall meet the following standards and requirements for applications developed by it for deployment by the State:

1. Application access to databases must be based on user credentials or service accounts.
2. Applications performing payment processing must do so through an interface with one of the State's contracted payment processors and the Contractor must meet all applicable and relevant PCI DSS security requirements.
3. The Contractor must complete a comprehensive source code scan (using guidance from SANS, OWASP, and other nationally or internationally recognized sources) of all applications on an annual basis. The Contractor must review the proposed source code scan methodology with designated State security staff members before use of the methodology to complete the source code scan. Upon request, the results must be delivered to and reviewed with the State.
4. The Contractor must use the Web Accessibility Initiative's (WAI) Web Content Accessibility Guidelines (WCAG) 2.0, Level AA (ISO/IEC 40500:2012), which reflect administrative rules on IT accessibility.
5. For applications that may involve information having a security classification by the Department of Defense, the State may request the Contractor to consult and follow the Security Technical Implementation Guides ("STIG") from the Defense Information Systems Agency ("DISTA"); the parties will develop an appropriate Statement of Work incorporating the agreed-upon methodology on a case-by- case basis.
6. The Contractor and the State will identify the appropriate controls to perform from the Information Assurance Support Environment (IASE) STIGs Application Security & Development for all major application changes to existing applications and new application developments where the application contains sensitive data or as requested by the State.
7. As required on a project basis, the Contractor's products and services shall be compliant with Section 508 of the Rehabilitation Act of 1973 ("§ 508"), which shall be documented by internal accessibility policy documents and accessibility testing documentation.
8. As required on a project basis, the Contractor's applications shall use TLS, conforming to IOT's TLS encryption standards, to protect data containing protected health information as defined in the Health Information Technology for Economic and Clinical Health Act, user credentials, (username and password), credit/debit card numbers, checking account and routing numbers, and personal information as defined by Ind. Code§ 4-1-6-l(b), Ind. Code§ 24-4.9-3, and Ind. Code§ 9-14-13. IOT's TLS standard will inform the Contractor as to which versions of TLS are approved, the algorithms and key lengths approved for server authentication, and the algorithms and key lengths approved for session protections.
9. All supported applications must be cross-browser compatible.

1.14.2 Application Methodologies, Processes, and Tools

Contractor, IOT and IOT State Entity Users shall discuss and support the appropriate development methodology to be utilized with respect to each Application maintained and used by IOT and State Entity Users. IOT retains the right to mandate the methodology to be utilized.

1.14.2.1 Processes and Tools

Contractor shall:

1. Document and refine application development methodologies for IOT's review and approval
2. Create methods, processes, and procedures for IOT's review and approval
3. Coordinate implementation of methods, processes, and procedures
4. Use source control tools to store and manage software builds and releases throughout the software development and maintenance lifecycle

1.14.3 Application Programming and Development Standards

The Contractor shall be responsible for the security and integrity of all applications it develops for deployment by the State. The Contractor must:

1. Conform to applicable industry practice in its application development. All applications must be developed based on secure coding guidelines such as the Open Web Application Security Project Guidelines ("OWASP") Top 10 and the CWE/SANS Top 25 Programming Errors published regularly by the SANS Institute.
2. Use application scanning software and a process to promote the release of secure code at the time such code is put into production.
3. Use commercially reasonable efforts to implement appropriate changes needed as a result of updates published to the guidelines.
4. Adhere to all applicable Standards (State, SOX and PCI DSS) for all Application Development. Should the State request access to any data covered by PCI DSS, then State compliance with PCI DSS requirements is a necessary pre-condition to Contractor compliance.
5. Use commercially reasonable efforts to ensure that the hardware, software and services provided to or purchased by the State from the Contractor are compatible with the principles and goals contained in the electronic and information technology accessibility standards adopted under Section 508 of the Federal Rehabilitation Act of 1973 (29 U.S.C. 794d).
6. Conform to Information Assurance Support Environment (IASE) STIGs Application Security & Development for all major application changes to existing application and new application development devours.

1.14.4 Application Release Control

The Contractor shall:

1. Perform all functions required to maintain the current applications environment
2. Perform all application modifications, testing, and acceptance testing needed
3. Assume full responsibility for release packaging and project commitments for the Applications as in the mutually agreed to release procedures
4. Support and adhere to IOT's process for priority setting, planning, and scheduling of Releases
5. Monitor the release schedule, and report all schedule exceptions to IOT as required by the Change Management and the Release and Deployment Management processes as outlined in Section 1.3 Program Management, Change Management and Release Control.
6. Provide the necessary interfaces during the development, testing and implementation phases.
7. Maintain source code and version control in the Contractor-provided Code Database.
8. Perform malware scanning and eradication on new and modified Software and document the results of such scan and eradication

9. Coordinate the planning and scheduling of all upgrades with IOT
10. Promptly report to IOT any audit compliance issues or e-discovery issues when such issues become known to Contractor

1.14.5 Application Development Project Initiation

Application Development projects can be initiated by IOT or a State Entity User to the Contractor directly or through the Webmasters.IN.Gov service request system. All projects must be approved by IOT before the Contractor engages.

All projects shall follow a process based on the IOT Project Development Life Cycle as outlined in Section 1.3.4.1- Project Development Lifecycle. With IOT approval, the Contractor may implement its own processes, or modify IOT's processes, to fulfill its obligations to the State.

Application Development shall include the following activities:

1. Development Estimation
2. Application Design
3. Application Coding
4. Removed
5. Cross-boundary Application Development
6. Cross browser compatibility
7. Application Maintenance
8. Unit Testing
9. Load Testing
10. Change Orders
11. Adherence to applicable Standards (State, PHI, PII, Section 508, SOX and PCI DSS)
12. Requirements gathering and implementation

1.14.6 Application Repository and Source Code

As part of Baseline Services, the Contractor must build and maintain an applications and services library where the data is backed by a data store and is manageable online. This library must list all applications used in connection with IN.gov and be designed to grow over time. It shall contain any project portfolio metadata applicable to an application, module or service, such as name, version, where deployed, connection strings, contact persons, description, applicable dashboard pages, and hyperlinks to dependencies when possible. The applications inventory data must be housed via an online database with the backend database hosted at IOT. It must be audited and updated no less than quarterly and readily accessible by the State. The Contractor must work with the State to determine the metadata needed and provide a redesigned Repository within 6 months of a signed Contract.

For each new or updated application, the Contractor must update the applications repository, including key metadata.

All applications must be developed to take advantage of and maximize code reusability, such as for login and Enterprise Service Bus (ESB).

IOT shall maintain ownership of source code and documentation for developed applications. Contractor shall identify reusable source code appropriate for the repository and make available to IOT and IOT State Entity Users in the Contractor provided Code Database.

1.14.6.1 Application Source Code Security

Contractor shall:

1. Implement all security requests and password reset requests associated with applications code subject to IOT and State Entity User approval on all data or information requests
2. Install, when required, and maintain source control software in compliance with IOT's standards and methodology.
3. Monitor and restrict access to source code and IOT Data in accordance with IOT policies
4. Comply with Ad Hoc, annual audit, and regulatory requests
5. Perform IOT Data/source code security audits, and report test results
6. Immediately report any security violations to IOT
7. Promptly report to IOT any SSAE-18 compliance issues or e-discovery issues as such issues become known to the Contractor.

Contractor must create a security risk assessment for new and modified applications to identify potential threats and vulnerabilities and proposed prevention measures.

1.14.6.2 Code Repository

Contractor shall:

1. Enable and configure a tool to host IN.gov code associated with Developed Materials
2. Develop a method for State Entity Users to obtain and use the available code
3. Create and maintain a list with associated description of available source code
4. Publish updates with newly available code every quarter
5. Prior to code being added to the repository, the Contractor will conduct quality checks to ensure there are no outstanding defects that need to be corrected. The Contractor shall not be responsible for assisting State Entity Users with installation and troubleshooting once the State Entity Users has downloaded the code
6. If Contractor becomes aware of a defect after publishing source code Contractor will correct and republish with a note in the associated description that a new version has been published

1.14.7 Maintenance of Applications

All services and applications, whether developed as part of Baseline Services or as a Time & Materials Task Order, must be supported and maintained by the Contractor as part of the Baseline Services. Contractor shall build, execute and maintain plans to successfully and efficiently execute application maintenance procedures. This does not include application enhancements or change orders.

1.14.8 Maintenance and Operation of Existing Applications

The State and the Contractor have mutually identified certain existing applications that shall be supported and maintained by the Contractor as part of Future Work and in accordance with the rates outlined in Exhibit 2, Section II., Maintenance and Operation for Existing Applications. This work must be developed by the Contractor as a Task Order. Contractor shall build, execute and maintain plans to successfully and efficiently execute application maintenance procedures. These procedures shall be documented in a Statement of Work for each application identified below. Contractor shall also ensure the ability to procure services for the benefit of programs covered under this section is included as a part of maintenance and support. Each application will include the following:

1. Production hosting and 24/7 operational monitoring.
2. Disaster recovery environment with failover capabilities.

3. All network/datacenter protections (including but not limited to: DDoS, WAF, IPS, IDS, File Integrity Monitoring).
4. Contractor will continue to scan and patch each application for required security and dependency updates such as JavaScript libraries and .Net frameworks.
5. Contractor will continue to maintain the application framework and update as needed.
6. Contractor will provide day-to-day support and operations for each application.
7. Contractor will provide third-party uptime monitoring for each application.
8. Contractor will continue to enhance the applications, via Change Orders at rate card rates, by request.
9. Subject to IOT review and approval, Contractor will work with the State Agency to evaluate Tyler platforms that could be leveraged to replace the full-stack application. (Implementation, SaaS, and other fees will apply)

The State and the Contractor have identified the following list of existing applications that will be supported and maintained under this clause:

Application Name	Application Size/Complexity
IGC License and Application Management (LAM)	Extra Large
FSSA DEBS	Extra Large
FSSA ViewPoint	Extra Large
FSSA INconnect	Extra Large
FSSA Childcare Finder (part of INconnect)	N/A
IGC Electronic Tax System (ETS)	Large
FSSA INconnect Alliance	Large
FSSA AAA/ICM portal	Medium
IGC Internet Self Restriction Program (ISRP) aka Voluntary Exclusion Program (VEP)	Medium
ISC Clerk of Courts Portal	Medium
FSSA Suicide Prevention Map	Small
ILRC Lobbyist Registration & Public Search	N/A
ISP Bus Inspections	N/A

1.15 Third-Party Applications

1.15.1 Third-Party Applications – General

The Contractor shall keep all IN.gov-supported and hosted third-party, portal service applications current, shall monitor release announcements, perform software updates on a timely basis, adhere to all IOT security and Cloud policies, segment all third-party hosting from the network, and must maintain version control history and documentation for all IN.gov supported, third-party portal service applications. For the avoidance of doubt, third-party applications may also include Contractor or its affiliate's applications.

The Contractor shall provide the integration and management of all necessary third-party applications as part of Baseline Services, unless expressly provided by the State Entity User. Where Third-Party State Entity User Managed applications are required, the Contractor shall be responsible for the integration as part of Baseline Services.

Third-Party Portal Managed applications required in support of the following IN.gov functionality include:

- Calendar & Events Registration
- Accessibility and Quality Assurance
- Accessibility Screen Reader
- Automated Web Accessibility Tool
- URL Shortener Custom App
- Content Management System
- Website Search Tool
- Website Analytics
- Mapping Development Tool for Web Development
- FAQ Solution
- Chat Bot and Live Chat Solution
- User Testing
- Web-based Org Chart Solution
- Form and Workflow Builder and Management Solution
- Mobile Application Solutions
- Subscription Service for Website Stickers and Icons
- Application Style Guide
- Standard Application Header
- Training for all Third-Party Applications or First-Party Solutions

Contractors shall adhere to the following requirements regarding software ownership and maintenance:

1. Where software is existing and licensed by the State, the State will continue to retain ownership until current software contract expiration, at which time it will be the responsibility of the Contractor to provide the required licenses as part of Baseline Services if such software is determined to be the best proposed solution by the Contractor. Maintenance, in accordance with existing agreements, and management of the software shall be the responsibility of the Contractor until the transition of complete Contractor ownership occurs. During the initial implementation phase, the Contractor shall provide a calendar outlining required license ownership transition.

2. Where software or future software that is required as a part of the Contract and has not been procured directly by the State, the Contractor must acquire these services as part of Baseline Services. The Contractor shall retain ownership and responsibility for these licenses. During the life of the Contract the management and maintenance of the software shall be the responsibility of the Contractor.

3. The State retains all rights to the underlying State data and reports contained in these software elements;

4. As part of a yearly State Entity User Technology Needs Assessment/Support review, the Contractor must look for and identify potential tools and/or technologies that could meet the needs of multiple State Entity Users. As part of Baseline Services, the Contractor

shall review with IOT annually and add 3rd Party applications as mutually agreed upon.

5. On occasion, the Contractor may be requested to procure additional third-party solutions outside the scope of Baseline Services for the benefit of IN.gov. When this occurs, it shall be agreed to by both parties, documented via Task Order, and invoiced to the State.

6. The Contractor must develop, maintain, execute, and publish a plan to reduce technical debt and increase adoption of service-based capabilities.

1.15.2 Third-Party Application Hosting

1. The Contractor, in conjunction with IOT IN.gov, shall review State Agency requests for third-party applications. Upon approval by IOT IN.gov and the Contractor, the Contractor and IOT IN.gov shall provide the requirements and specifications to the third-party application provider. The Contractor shall test applications provided by third parties and proposed for deployment on IN.gov for the limited purpose of determining whether they appear to conform to IN.gov deployment standards. Baseline testing of third-party applications will be for hosting or enterprise service interface compliance only. More detailed testing or conversion of applications can be performed as part of Baseline Services, as needed. The Contractor will not perform any testing beyond that which is required to determine whether a third-party application appears to meet the published standards for hosting within the Contractor's hosting environment. Contractor testing does not in any manner make the Contractor responsible for the performance of third-party applications or their effect upon IN.gov once deployed.
2. The Contractor shall provide infrastructure support and coordination for third parties that may deliver an application in order to leverage a Contractor-deployed enterprise service, such as payment processing on IN.gov. The Contractor shall provide consulting on how to interface with any of the Contractor's enterprise services, but shall not customize or change those systems or services to interface with a third-party application.
3. The Contractor shall provide communications and hosting support for any Contractor-built service that interfaces with, or utilizes, a third-party application. The Contractor shall cooperate with other vendors that may provide those third-party back-end systems to make the Contractor's systems compliant with other third parties. If a Time & Materials project requires an interface to a third-party application, the Contractor shall price the support and communication utilizing the Future Work Rate Card.
4. The Contractor shall not be responsible for the internal functioning of third-party software or its effect upon the portal.

All other State Entity User customers shall be given the option of Contractor hosting or IOT hosting for their individual Third-Party State Entity Managed Applications and it shall be entirely at the discretion of individual State Entity Users. In the event a State Entity User elects Contractor hosting, the Contractor shall bill the State Entity User directly using a Task Order and the pricing in Exhibit 2- Pricing. Exhibit 13- RFP & Response Suite of Documents includes Current Third-Party Hosting Requirements and outlines the Baseline included for State Entity User paid hosting requirements.

Support activities shall be provided for both Third-Party Portal Managed Applications and Third-Party State Entity User Managed Applications. In order to facilitate supporting the third-party

applications on the hosting environment, the State agrees to require that third-party application developers develop the application in a way that eases integration, by adhering to IN.gov development and hosting standards promulgated by the State and mutually agreed upon by the Contractor and the State. The Contractor shall not be required to modify third-party software.

1.16 Data Management

The Contractor must develop or provide a system that can manage the data sales and management program for the State including user transactions with the State of Indiana and user accounts associated with those transactions. The Contractor shall also manage applications associated with the data sales system(s) and manage State of Indiana State Entity Users' access to the system(s).

In executing data management and sales duties under this Contract, the Contractor shall adhere to all relevant State (e.g., IC 4-5-10-1, IC 5-14-3-3.5, IC 9-14-13-7; 9-14-13-8, 9-14-13-9, and 9-14-13-10) and federal (e.g., the Drivers Privacy Protection Act) regulations, statutes, laws, and policies.

1.16.1 Account Database As part of the Baseline Services, the Contractor shall maintain an Account Database, using the State's authentication solution, that permits account maintenance, creation, verification, authorization, and invoicing functions. The Contractor shall set up user IDs enabling the State (including both IOT and other State of Indiana State Entity Users) to access the Contractor's database.

The Account Database or System shall contain a subscriber center that allows individuals and entities to subscribe to Web Portal premium services. Premium services include but are not limited to:

1. Anytime online access - 7 days per week, 24 hours per day with (the exception of scheduled maintenance or unforeseen outage).
2. Subscriber-only features such as ID Validate, online eFiling for Lobbyists, and Professional License watch
3. The ability to select how you pay - monthly billing or auto-pay
4. Track usage with the ability to view and print statements and invoices

The Account Database must have mechanisms to log and bill transactions (including for auto-payment users), track recurring transactions, generate and distribute invoices, develop transaction memos ~~(~~and tie them to user IDs~~)~~, reconcile payments, and authorize users for application use.

The user interface of the Account Database or System shall be responsive with a consistent uniform interface.

The State's Single Sign On Enterprise Authentication standard (SSO) will be used to authenticate users and handle certain account maintenance functions such as password resets. The Contractor, at its sole expense, shall expeditiously take the necessary steps so that the Account Database is compatible and functional with the State's solution. The form of the account agreement, user verification requirements, and security and access levels for various applications shall be agreed upon by the State and the Contractor in a Scope of Work. The

Contractor may inform the State if it becomes aware of changes or modifications to the account agreements, user verification requirements, or security and access requirements that would improve services offered.

The Contractor shall collect information from end users, transmit the information to the payment processor or bank, and make certain agreed-to data and information available for review by the State via the Contractor's reporting tools to support disbursements to the proper State Entity User accounts. As part of the Baseline Services, the State, through the Contractor, shall benefit from any replacements or enhancements to any currently utilized Account Database or System that are generally made available during the term of this Contract. Should the State request IN.gov customizations to the Account Database that the Contractor agrees should be incorporated, such customizations will be performed on a Task Order basis.

1.16.1.1 Account Management

The Contractor shall be responsible for establishing, verifying, and maintaining user accounts for individuals or entities entering into account agreements for IN.gov. The Contractor shall also manage all subscriptions, including contracts with subscribing entities and third-party contracts related to Account Database data.

Additional responsibilities of the Contractor include, but are not limited to:

1. Account setup and maintenance
    - Account creation, enabling/disabling users, and general user management
2. Generating user IDs and account-related communication to users
3. Ensuring anonymous or unknown accounts are prevented from gaining access to data (e.g., a user with no identifying information cannot access or receive data)
4. Maintenance of hard-copy files containing original, signed data sales user contracts
5. Customer billing questions
6. Credit card expiration date tracking and maintenance
7. Management of government monthly accounts (State Agencies have free access to most portal services, but must maintain a monthly account to capture users obtaining access to services)
8. Implementation of the State's determination of which users should have access to which systems/services
9. Customer service processes to initiate the State's collection efforts for portal monthly accounts, which currently bill in arrears of portal service usage
10. Fielding general user requests from companies, individuals, government agencies, qualifying academic and educational entities pertaining to data sales or the Account Database

1.16.1.2 Access Types

1. *Guest Access:* Guest Access allows users to make purchases without creating an account (note: users still need to provide basic identifying information). For example, an individual can utilize Guest Access to purchase a copy of a driving record. Regardless of whether the user creates an account, the user still must be shown a screen that outlines rules of the data management and sales program and relevant statutes prior to making any purchases.

2. *Subscriber Access:* Subscriber Access is utilized by individuals and entities that have an IN.gov account and pay recurring fees in addition to per transaction fees. Users with subscriber access have signed an agreement with the State allowing them to access data. Subscriber Access is divided into two sub-group access levels: Basic Subscriber Access and Enhanced Subscriber Access. Basic Subscriber Access allows individuals and entities to access a limited subset of data based on State Entity User-set parameters, while Enhanced Subscriber Access allows individuals and entities to access all data related to a user request. Enhanced Subscriber Access normally requires users to provide verification that they are eligible to receive special access for data related to a user request.
3. Batch Data Access: Batch Data Access is leveraged by users seeking to directly receive data on a large scale. Users are sent data via a batch and then periodically receive updates to that data at varying cadences (e.g., weekly, monthly).
4. Real-Time Data Access: Real-Time Data Access is leveraged by users who seek a direct API to State Entity User systems. Changes to data are automatically reflected, so users do not need to rely on period batch updates to view the changes. Some Real-Time Data Access users may seek access to all accessible data in the data management and sales program.

The Contractor shall be responsible for onboarding users. User's requesting Batch Data or Real-Time Data Access must be properly vetted and have direct approval from the state to be granted access.

1.16.1.3 User Authorization Procedures

When a user submits an application to become an IN.gov subscriber and pays all necessary fees, the Contractor shall grant the user authorization.

For authorization levels that require special access, the Contractor must ensure the Account Database restricts user access to that data until the special access has been granted by the State. The Contractor must vet users seeking special access to ensure they meet the data management and sales program requirements and present their evaluations and recommendations to the State. The Contractor shall log all research conducted to vet a user and shall, upon request by the State, make available all documents that were factored into an authorization decision. The State is ultimately responsible for communicating which users shall be granted access to data and at what level, based on the Contractor's recommendations.

Once users are granted authorization, the Contractor shall proactively monitor and evaluate users on an on-going basis to ensure adherence to all data management and sales program requirements and State and federal regulations.

In the case of employee termination or the requirement that access to the system no longer be granted, the State is responsible for promptly identifying the necessary information to the Contractor.

If a third-party would prefer to have a direct agreement with the State, the third-party will apply for an Account Database user ID and execute an agreement with the State (if not already

completed). Once executed, the State will then send the agreement to the Contractor. At that point, the Contractor shall permit access to data and manage invoicing unless otherwise directed by the State.

1.16.2 Account Database Reports

The Contractor shall develop data sales and management-specific reports for both IOT and State Entity Users. In addition, the Account Database shall allow for the viewing of transaction-level detail and reports by State Entity User and/or service.

The Contractor shall submit a quarterly report to the State. This report must contain the following:

1. State Entity User specific breakdowns of data sales
2. Results of quarterly account audits
3. New bulk data and subscription requests that will be voted on by the Committee (Note: new bulk data and subscription requests may still be submitted outside of this quarterly report)
4. Other information as directed by the Committee

The Contractor shall also provide data sales information as well as regional/national fee structure information to the Enhanced Data Access Records Committee.

1.16.3 Data Management and Sales Integrity and Auditing

The Contractor shall proactively take measures to monitor and ensure the integrity of the data management and sales program. The Contractor must alert the State to any data management and sales program or Account Database irregularities, risks, or issues as soon as they are discovered.

The Contractor shall proactively monitor for breaches and misuses of data. If a breach or instance of data misuse occurs, the Contractor shall adhere to the Disclosure of a Security Breach Protocol outlined in Section 1.10.12- Disclosure of a Security Breach. The Contractor shall also ensure that all data buyers are held responsible for any breach or misuse of data by themselves or any entity that they sell or distribute data to.

The Account Database shall be fully auditable, keeping track of all user actions, transactions, and data pulls, including details on who performed certain actions, when actions occurred, and any dollar amounts associated with the action. Upon request by the State, the Account Database shall develop user-specific action logs. The Contractor shall also develop audit tools that can be leveraged by individual agencies when requested.

The Contractor shall comply with all audit requests from the State pertaining to data management and sales. At a minimum, the State will audit account usage in alignment with State statutes and State Entity User requirements (on a quarterly basis) and the Contractor must include the results of this audit in their quarterly report to the State. In addition, the State reserves the right to: directly audit the Contractor with or without advanced notice, directly audit data purchasers with or without advanced notice, require third party auditing, control onboarding

criteria for all programs, suspend users who fail to meet program requirements, and suspend users or programs upon an irregularity, such as a data breach.

The Contractor's Account Database must keep track of all defaulted or suspended users. Upon request by the State, the Contractor shall provide a list of all defaulted and suspended users.

1.16.4 Data Management and Sales Growth and Outreach

The Contractor shall employ growth strategies for the purpose of generating additional data management and sales program-related utilization and business. The Contractor shall work with the State to develop State Entity User-specific outreach plans and then manage the implementation of those plans. The Contractor's plans, strategies, and mechanisms must be clearly defined in the Contractor's Marketing and Outreach Plan (see Section 1.8 - Marketing for more information regarding this plan).

The Contractor shall ensure that materials sent to subscribers are able to contain inserts that the State can utilize for marketing purposes.

The Contractor shall aggregate and analyze its growth strategies and provide the State with results and plans for future improvement. Growth strategies will include, but are not limited to:

1. Increasing sales of existing services through strategic marketing campaigns. The objective of these campaigns will be to identify potential customers, market to those customers, and develop a sales lead pipeline that is managed by the Contractor and State Entity Users.
2. Identify new services to be introduced under the IN.gov Program. The Contractor will work with the State to identify datasets that have a valuable commercial use case paired with high demand that will assist the state in increasing its revenue.

The Contractor's staff will be trained to identify opportunities for new services to be presented to the State for approval. This training will include a review of all services the Contractor offers to its clients, and strategies to better understand the State's needs through discussions with State Entity Users.

1.16.5 Current State Entity User Specifics

Current State Entity User subscriber center services include:

1. Bureau of Motor Vehicles (BMV)
    a. BMV Driver License Requests
    b. BMV Registration Requests
    c. BMV Title Requests
    d. BMV Validate Fee
    e. BMV Point to Point Drivers' License Data (PTP DL)
    f. BMV Limited Registration Search
    g. BMV Digital Certified Drivers' License Record (DLR)
    h. BMV Commercial Drivers' License (CDL) Driver Monitoring Fee
    i. BMV CDL Monitoring Record Pull
    j. BMV CDL Driver Monitoring Annual Fee
2. Indiana Department of Child Services (DCS)

    a. Child Support Arrears Delinquency Registry (CSADR)
3. Indiana Department of Natural Resources (DNR)
    a. DNR Water Permit
4. Indiana Department of Transportation (INDOT)
    a. INDOT Miscellaneous Permit Fee
5. Indiana Lobbyist Registration Commission (ILRC)
    a. ILRC Employer Lobbyist Registration
    b. ILRC Compensated Lobbyist Registration
    c. ILRC Activity Filing
    d. ILRC Gift Reporting
    e. ILRC Amendment
    f. ILRC Employer Non-Profit
    g. ILRC Employer Compensated Existing
    h. ILRC Comp Code Non-Profit
    i. ILRC eFiling Late Fee
    j. ILRC Compensated Employer Existing
    k. ILRC Purchase Report Fees
6. Indiana State Police (ISP)
    a. ISP Limited Criminal History
7. Professional Licensing Agency (PLA)
    a. PLA License Verification
    b. PLA Digital License Verification
    c. PLA Bulk Download
    d. PLA Bulk Add Records
    e. PLA IN License Watch 1 -24
    f. PLA IN License Watch 25-100
    g. PLA IN License Watch 101-400
    h. PLA IN License Watch 401-1200
    i. PLA IN License Watch 1201-2000
    j. PLA IN License Watch 2000 up
8. Miscellaneous
    a. The authorization module is used to provide authorization into various websites (this will eventually be replaced with Access Indiana).

The Contractor shall be responsible for the maintenance of the above subscriber center services. Upon request by a State Entity User and approval by IOT, the Contractor must modify or develop new subscriber center services at no additional cost to the State.

1.16.6 Invoicing, Fee Handling, and Annual Subscription Fee

The Contractor shall be responsible for processing monthly invoices and billing all account users each month. The Contractor's Account Database shall aggregate all fees and transactions processed. As part of this aggregation, the Contractor's Account Database must clearly define the user who completed the transaction, what transaction was completed, and the total amount due for the transaction. At the end of each month, the Contractor must generate and send invoices electronically.

The State's payment processing vendor(s) will collect (via online or through the mail) and pass through to the State (via a deposit into the State's account) any fees associated with subscriber

accounts. The account fees are comprised of an annual subscription fee and monthly invoices based on the total number of transactions for each account.

The Contractor's Account Database shall integrate with the State's payment processing vendor(s) and their system / technologies. The Contractor shall be responsible for working with the State's payment processing vendor(s) to process account payments made by EFT or credit cards, disbursing such funds to the depository designated by the Treasurer of State, and providing reports on all disbursements.

During the term of the Contract, the Contractor will work with the payment processing vendor(s) to ensure the collection (and the pass through to the State) of an annual fee of up to $95.00 to users establishing or renewing an account for IN.gov. Reduction or waiver of this fee for government-funded entities shall be granted upon the State's request and pursuant to applicable law. Any changes to the annual fee will be determined by the State. The Contractor shall be responsible for coordinating with the State's payment processing vendor(s) to the extent necessary to ensure annual fees are paid and passed through to the State.

The Contractor may suspend or close the account of any customer who has not paid the annual or monthly fees when due.

The Contractor shall provide a monthly Account Receivable report to the State for outstanding monthly account payments due to the State from both State Agencies and private monthly account customers.

The Contractor shall use the below guidelines with regard to contacting any past due non-governmental monthly account customer. An account shall be deemed past due when payment has not been received by the time called for in the Account Agreement. The Contractor is not responsible for any uncollected amounts.

The Contractor shall take the following actions according to the designated numbers of days following the issuance date of any invoice:

1. 30 days- Check lockbox or system information for recent payments processed, put any appropriate accounts on watch list if payment is not received, and alert account holder of overdue status via a second billing notice.
2. 60 days - Check lockbox or system information for recent payments processed, suspend access to the portal for any appropriate accounts if payment is not received, make a courtesy call to the account holder's phone number of record to notify the monthly account holder of their suspended status and the necessary process to get the account holder's service reinstated.
    A. If the Contractor reaches the account holder's voice mail, the Contractor shall leave a message.
    B. If the Contractor is unable to leave a message, speak with the account holder or if the phone number of record is wrong, the Contractor shall continue to follow the process defined in the bullet below.

3. 90 days - Refer to the State for collection. Move account from suspended to closed. If contacted about resuming service, explain that account holder must:
    A. Bring account balance current,
    B. Remit new annual account fee, and make prepayment for ongoing services, if required by State.

Once the information has been referred to the State for collection, the Contractor has no further obligation for the processing or attempted collection of past due amounts. The Contractor makes no guarantee of payment or collection for any portal services rendered.

1.16.6.1 Credit Balance Reports

The following reports regarding customer account credit balances on the books for 90 days or longer shall be submitted to IOT by the 15th of each month:

1. List of all closed accounts having a credit balance of less than Five Dollars ($5.00). Upon instructions from IOT, the Contractor shall clear out such accounts by debit memo.
2. List of all closed accounts having a credit balance in excess of Five Dollars ($5.00). The Contractor shall pay the credit balance to the customer and bill IOT for that amount.
3. List of all active accounts having a credit balance of greater than $100 for the past quarter. The Contractor shall bill IOT for the credit balance and shall remit the credit balance to the customer upon payment by IOT.
4. The Contractor shall make the payments required above before the next monthly report is made.

1.16.6.2 Transaction Fees

Transaction fees are charged per service. All transaction fees are to be collected and passed through directly to the State.

All per-transaction charges shall be in accordance with the then-current IN.gov account agreements and applicable service schedules, and shall be subject to applicable sales and use taxes, which taxes may be charged by the Contractor in addition to the agreed-to per-transaction charges.

1.17 Quality Assurance

The Contractor must have a dedicated Quality Assurance (QA) team, including a dedicated Analyst. The Contractor is responsible for developing and establishing quality assurance standards and measures for the information technology services within the Contractor's organization for the IN.gov Web Portal. The Contractor shall also gather and analyze data in support of business cases, proposed projects, and systems requirements for the IN.gov Web Portal. This shall include designing test plans, scripts and regression suites for testing during development and user testing. The Contractor shall be responsible for tracking defects and fixes both during development and post deployment.

In addition to testing applications developed by the Contractor, the Contractor must maintain a test environment for testing all IN.gov-supported third-party Application updates and upgrades prior to release.

For the IN.gov portal and applications developed by the Contractor, the Contractor will:

1. Develop and establish quality assurance measures and testing standards for new applications, products, and/or enhancements to applications throughout their development/product life cycles
2. Analyze documentation and technical specifications of any new application
3. Conduct internal audits to measure and assure adherence to established QA standards for software development, application integration and information system performance, and corresponding documentation
4. Create and execute test plans
5. Perform testing activities that demonstrate whether applications meet business requirements
6. Collaborate with software/systems personnel in application testing, such as system, unit, regression, load, and acceptance testing methods
7. Communicate test progress, test results
8. Test any new software with respect to functional requirements, system compliance, and technical specifications
9. Analyze formal test results with respect to defects, bugs; errors, configuration issues, and interoperability flaws
10. Assist in the development of change control processes, practices, and guidelines for new and existing technologies

1.18 Initial Transition

Prior to taking over the Scope of Work noted in this Contract, the Contractor shall work with the State to develop and manage an Initial Transition Plan. The Initial Transition Plan must include a comprehensive list of all Contractor start-up activities and be approved by the State. The Contractor shall oversee the successful implementation of the Initial Transition Plan. The schedule and activities may be subject to adjustments made collaboratively by the Contractor and the State.

The Contractor shall complete the following tasks and activities during the Initial Transition period:

1. Develop an Initial Transition Plan, subject to State approval, including a detailed schedule and resources (quantity, type, and role) who will be available for all months of the Initial Transition.
    a. The Initial Transition Plan shall outline the following:
        i. An initial Resource Usage Guide that includes Contractor roles and responsibilities, including the roles and responsibilities of any subcontractors

ii. Contractor point(s) of contact
iii. A schedule with key milestones and deliverables, including
- Completion of a full evaluation of reporting deliverables under the contract
- Completion of a full evaluation of SLA requirements to define a set of standard operating procedures for the various events identified within the contract
- Identification of the core team to meet the contract requirements
- Conducting a thorough needs assessment, collaborating closely with IOT and State Entity Users to understand business requirements and desired outcomes.
- Conducting an extensive market analysis to identify software solutions relevant to The States needs
- Assessment the pros and cons of identified software solutions
- Technical analysis of the identified software solutions
- Creating a recommendation for implementing a pilot test(s) of identified software solutions

iv. A schedule and cadence for Initial Transition meetings and post Initial Transition operational meetings with the State
v. State team roles and responsibilities
vi. Contractor methods, mechanisms, and procedures that will be utilized to complete the transition
vii. Issues and risks that need to be addressed during the transition period

2. Creation of transition meetings with the State to execute the Initial Transition Plan
3. Ensure complete turnover of all in-progress artifacts and solution components.
4. Confirm full administrative edit access to all environments for appropriate staff.
5. Complete all activities in the Initial Transition Plan.

1.19 End of Contract Turnover

The Contractor is responsible for planning and performing end of contract turnover and disengagement activities. Disengagement includes transition planning to ensure a seamless operational transition to the State or its designee in the event of required contract transition. The Contractor shall work with the State to assure that all end of contract turnover tasks are completed and that all responsibilities are transitioned in a timely and effective manner.
The Contractor shall complete the following tasks and activities during the End of Contract Turnover period:

1. Develop an End of Contract Turnover Plan, subject to State approval, including a detailed schedule and resources (quantity, type, and role) who will be available for all months of the End of Contract Turnover period.
    a. The End of Contract Turnover Plan shall outline the following:
        i. Contractor roles and responsibilities
        ii. State roles and responsibilities
        iii. A schedule with key milestones and deliverables
        iv. Method to transfer information to the State and/or a successor contractor(s)

v. An inventory of detailed documentation about operations, applications, architecture, and infrastructure, as well as any supporting information related to the technical architecture and infrastructure.
vi. An inventory of all work-in-progress that need to be completed by the State and/or a successor contractor(s)
vii. Plans for coordination and transition of specific responsibilities from the incumbent to the future contractor.
viii. An inventory of all relevant project artifacts created, maintained, and updated throughout the Contract term
ix. An inventory of project documentation, work-in-progress, technology, systems, and assets necessary for a successive Contractor to perform the duties of the Scope of Work
x. An inventory of third-party products, software, and vanity URLs for which the licenses need to be transferred

2. Conduct training of State staff or successor contractor(s) staff, in the operations and procedures performed by Contractor staff.
3. Perform shadowing and training activities for the State and successor contractor(s)
4. Transfer the following information to the State or a successor contractor(s) on a medium acceptable to the State:
    a. All relevant project artifacts created, maintained, and updated throughout the Contract term
    b. Project documentation, work-in-progress, technology, systems, and assets necessary for a successive Contractor to perform the duties of the Scope of Work
    c. Other documentation including, but not limited to:
        i. User, provider, and operations manuals
        ii. Training materials
        iii. Documentation of any interfaces developed to support business activities between contractors
5. Participate in reverse shadowing for the State and/or successor contractor(s) staff on all aspects of workflows, releases, and assignments as requested by the State
6. Be available to provide support as requested by the State

By the end date of the Contract, the Contractor must turn over all State property to the State, and Contractor's access to all State infrastructure and facilities shall be terminated.
The State has the right to initiate the disengagement process for any service under the Contractor Scope of Work with thirty (30) calendar day's written notice. The notice of termination initiates these disengagement activities and responsibilities.

1.19.1 Data Center Turnover and Continuity
If this Contract expires or is terminated, and IN.gov is hosted by a third-party at the time of termination or expiration, the State may enter into a separate agreement for the continued use of the Data Center. Contractor's agreement with the Data Center shall contain a provision allowing the assignability of Contractor's agreement to the State in the event the Contractor is no longer providing portal services to the State. The agreement shall also include provisions for

the cooperation and reasonable assistance to the State in transitioning the service to the State. The Contractor warrants and represents that it has reached agreement with any third-party responsible for hosting with respect to these obligations.

Exhibit 2

Contract #79743 IN.gov Web Portal Exhibit 2
- Pricing
I. Baseline Services

The pricing defined in this Exhibit is agreed to in acknowledgement of, and assumption of adherence to, the information provided in Exhibits 2.5 - Cost Proposal Narrative and 2.6 - Cost Assumptions, Conditions and Constraints.

The annual Baseline Services prices, quoted under this Contract, shall be the fixed annual fees that the Contractor will bill the State over the course of each stated year to fund Baseline Services, as defined in Exhibit 1 - 1.1.3.1. The Contractor shall submit an invoice to the State requesting payment of the Baseline Services on a monthly basis. The below fees include Baseline Services for all State Agency Users and Political Subdivisions.

Baseline Services shall include the below annual Web Portal support elements. Any unused quantities shall carry forward into the following fiscal year. All quantities must be utilized prior the close of this Contract. In the event quantities are unable to be utilized, IOT and the Contractor shall determine a mutually agreed upon refund for all remaining quantities.

Proposed Hosting Solution	**Select One Option** On-Premise Hosting

	TOTAL ANNUAL PROPOSED PRICE - Contract Year 1	**TOTAL ANNUAL PROPOSED PRICE - Contract Year 2**	**TOTAL ANNUAL PROPOSED PRICE - Contract Year 3**	**TOTAL ANNUAL PROPOSED PRICE - Contract Year 4**	**TOTAL ANNUAL PROPOSED PRICE - Initial Contract Term**
Annual Baseline Services Price	$ 5,450,000.00	$ 5,599,875.00	$ 5,753,872.00	$ 5,912,103.00	$ 22,715,850.00

IN.gov Web Portal Support Elements	**Baseline Included Annual Quantity**
Baseline Services shall also incorporate a mutually agreed upon level of the following Web Portal support elements. Any unused quantities shall carry forward into the following fiscal year. All quantities must be utilized prior to contract close. In the event quantities are unable to be utilized, IOT and the Contractor shall determine a mutually agreed upon refund for all remaining quantities. Respondents shall propose an annual quantity in whole numbers for each IN.gov Web Portal Support Element listed:	
The addition of new Third-Party Portal Managed Applications	1
The addition of domain names	200

Contract #79743 IN.gov Web Portal
Exhibit 2 - Pricing
II. Future Work

Project Management Standard Resource Rates:

The standard hourly rates quoted under this Contract shall be for the design, development, testing and deployment of new applications, capabilities or significant application or capabilities enhancements not included within Baseline Services but still within the scope of this Contract ("future work").

Future work shall be mutually agreed upon by IOT and the Contractor and shall be documented using a Time and Materials Task Order (TO). State Entity Users may request additional work to be performed under this Contract via a TO.

The Contractor may not propose rates in any Time and Materials Task Order that exceed this rate card. The quoted maximum rates shall remain consistent for the life of the contract, including renewals.

Project Management Standard Resource Rates	Maximum Rate/Hr.	Job Summary
System Architect	$ 200.00	Design and implement complex IT systems, combining hardware, software, and networking components to meet business requirements while ensuring scalability, reliability, and security. 10 years of experience is preferred.
Senior Project Manager (PMP; > 3 years experience)	$ 150.00	Lead and oversee large-scale IT projects from initiation to completion, ensuring timely delivery, effective resource allocation, and stakeholder communication while managing risks and maintaining project quality. 4 years of experience is preferred.
Intermediate Project Manager (<3 years experience; has or is working towards PMP)	$ 125.00	Assist in managing IT projects, coordinating teams, tracking progress, and ensuring adherence to project plans and schedules to achieve successful project outcomes. 3 years of experience is preferred.
Enterprise Content Management Analyst	$ 100.00	Analyze, design, and implement enterprise content management solutions, including template design and development, document migration and storage, and workflow processes, to optimize information organization and accessibility. 3 years of experience is preferred.
Senior Developer	$ 175.00	Lead a team of developers in creating software solutions, utilizing best coding practices and technologies to deliver high-quality applications that align with business goals. 5 years of experience is preferred.
Senior Developer .NET	$ 175.00	Develop, test, and maintain .NET-based applications, collaborating with cross-functional teams to deliver efficient and reliable software solutions. 5 years of experience is preferred.
Senior Developer Java	$ 175.00	Develop, test, and maintain Java-based applications, collaborating with cross-functional teams to deliver efficient and reliable software solutions. 5 years of experience is preferred.
Intermediate Developer	$ 150.00	Contribute to the development of software applications, participate in code reviews, and troubleshoot technical issues to support the delivery of functional and optimized software. 3 years of experience is preferred.
Intermediate Developer Java and .NET	$ 150.00	Contribute to the development of software applications using both Java and .NET technologies, ensuring seamless integration and efficient functionality. 3 years of experience is preferred.
C# Developer	$ 150.00	Create, modify, and maintain C#-based software applications, focusing on clean code, efficient algorithms, and system performance. 3 years of experience is preferred.
Senior UI/UX Developer	$ 175.00	Design and implement user interfaces with a user-centered approach, ensuring intuitive and visually appealing experiences in alignment with business and user requirements. 5 years of experience is preferred.
Senior UI/UX Developer with Animation Skillset	$ 175.00	Enhance user interfaces with engaging animations, creating visually captivating and interactive user experiences to improve overall application usability. 5 years of experience is preferred.
Oracle Database Developer	$ 175.00	Design, develop, and optimize Oracle database solutions, ensuring efficient data storage, retrieval, and integrity within IT applications. 3 years of experience is preferred.
MS SQL Database Developer	$ 175.00	Develop and manage MS SQL database solutions, implementing effective data structures, querying, and optimization techniques to support software applications. 3 years of experience is preferred.
Java Developer	$ 150.00	Contribute to the development of Java software applications using both Java and .NET technologies, ensuring seamless integration and efficient functionality. 3 years of experience is preferred.
Test Coordinator	$ 150.00	Coordinate testing efforts, develop test plans, and oversee the execution of testing activities to ensure the quality and functionality of IT systems. 3 years of experience is preferred.
Tester	$ 125.00	Perform thorough testing of software applications, identify defects, and provide detailed feedback to developers to ensure the delivery of reliable and high-quality software. 2 years of experience is preferred.
Technical Writer	$ 100.00	Create clear and comprehensive technical documentation, including user manuals, guides, and specifications, to facilitate the understanding and usage of IT solutions. 3 years of experience is preferred.
Website Designer	$ 100.00	Design and develop visually appealing and user-friendly websites, applying web design best practices and coding languages to deliver effective online platforms. 3 years of experience is preferred.
Creative Website Designer	$ 100.00	Combine artistic creativity with technical expertise to design innovative and visually striking websites that captivate users and convey brand identity. 3 years of experience is preferred.
Business Analyst	$ 150.00	Analyze business processes, gather requirements, and translate them into IT solutions, bridging the gap between business needs and technology implementation. 3 years of experience is preferred.
Senior Quality Analyst	$ 150.00	Lead quality assurance efforts, establish testing standards, and ensure the delivery of error-free software solutions through rigorous testing and quality control. 4 years of experience is preferred.
Quality Analyst	$ 125.00	Conduct thorough testing and quality checks on software applications, identifying and reporting defects to contribute to the overall software quality. 3 years of experience is preferred.
Trainer	$ 100.00	Provide training and knowledge transfer to end-users, stakeholders, and IT teams on software applications, tools, and technologies, ensuring successful implementation and adoption. 3 years of experience is preferred.

Maintenance and Operations for Existing Applications:

The monthly rates quoted under this Contract shall be for the maintenance and operations (M&O) of certain existing apllications, defined in Exhibit 1 - 1.14.8. Maintenance and operations shall be performed as part of future work and documented using a Task Order.

The Contractor may not propose rates in any Task Order that exceed this rate card. The quoted rates shall remain consistent for the life of the contract, including renewals.

Size/Complexity	Monthly M&O Rate
Extra Large	$ 5,000.00
Large	$ 3,500.00
Medium	$ 1,500.00
Small	$ 500.00

Contract #79743 IN.gov Web Portal
Exhibit 2 - Pricing
III. Additional Pricing

The solution prices and considerations quoted under this Contract shall be included as part of Baseline Services for all State Entities or made available to State Entities via TO, based on classification.

	Proposed Solution	Pricing Considerations (# of licenses, etc.)	Pricing
Third-Party Portal Managed Applications (Baseline included for all State Entities)			
Calendar & Events Registration	Localist	Up to twenty-five (25) channels	$ 60,000.00
Accessibility and Quality Assurance	Siteimprove	Up to 85,000 pages	$ 75,000.00
Accessibility Screen Reader	Browsealoud	Can only be used on the www.in.gov domain	$ 12,000.00
Automated Web Accessibility Tool	AccessiBe	Can only be used on the www.in.gov domain	$ 20,000.00
URL Shortener	Tyler Technologies	N/A	$ 2,000.00
Content Management System	Squiz Matrix	Squiz Matrix 24/7 Service Level Agreement	$ 135,000.00
Website Search Tool	Funnelback	3,000,000 document limit	$ 105,000.00
Website Analytics	Google Analytics	up to 110M events/month	$ 150,000.00
Mapping Development Tool for Web Development (Note: the State's GIS tool will be the primary tool used for mapping)	MapBox	$6k for support business/$17k in credits to pay for service	$ 23,000.00
FAQ Solution	ZenDesk	N/A	$ 20,000.00
Form and Workflow Builder and Management Solution	Engagement Builder	Encompasses forms and workflows crafted by the user post-training	$ 50,000.00
Subscription Service for Website Stickers and Icons	iStock Photo	50 images/month	$ 1,200.00
Application Style Guide	Tyler Technologies	Utilization of existing Tyler Technologies solution	$ 2,000.00
Standard Application Header	Tyler Technologies	Utilization of existing Tyler Technologies solution	$ 2,000.00
Third-Party Portal Managed Applications (Baseline included for State Agencies only)			
Chat Bot and Live Chat Solution	ZenDesk	Serivce - Agency Quantity/month Support Enterprise - 17/month Advanced Security - 17/month Data Center Location - 17/month Chat Premium - 12/month Talk Basic - 8/month Explore Legacy - 17/month Gather Legacy - 17/month Guide Legacy - 17/month Sunshine Enteprise - 17/month Answer Bot - 300/month	$ 40,000.00
User Testing	UserTesting	Insight Core - Standard License (Prem Edition) 2/10 digital property bundle 1	$ 20,000.00
Web-based Org Chart Solution	Pingboard	Up to 50 users	$ 1,200.00
Mobile Application Solutions	MyCivic	1 Statewide branded implementation	$ 50,000.00
Third-Party State Entity Managed Application Hosting			
Hosting fee	Tyler Technologies	Includes 1 VM with standard configuration and assumes database is hosed by the Indiana Office of Technology	$ 2,400.00
Training and Support Services			
On-Site	Tyler Technologies	On-Site training at Tyler Technology and state government offices in Indianapolis are covered at no cost. On-site training at local government offices will vary based on distance travelled and agreed to in a statement of work or task order. Overnight stays will be billed per diem.	$ 75.00
Additional Support Service Requests	Tyler Technologies	Billed per hour based on the role needed to complete the support request. Training rate was provided as an example.	$ 75.00
Tyler Technologies Annual Conference Attendance	Tyler Technologies	Admission for up to four State Employees each year. Excludes travel expenses such as transportation and lodging	$ -

Contract #79743: IN.gov Web Portal

Exhibit 2 – Pricing
IV. Incentives and Value-Added Opportunities

The incentives and value-added opportunities, quoted below, shall be a mechanism by which the Contractor can earn additional revenue, beyond that associated with Baseline Services, by exceeding certain contractual requirements. Additional revenue paid to the Contractor is contingent upon meeting or exceeding the metrics defined below. Additional revenue earned upon meeting or exceeding the defined metrics will be paid to the Contractor on the invoice following the completion of the contract year. The first opportunity for the Contractor to be paid additional revenue shall be following the contract period from October 2024 – September 2025.

At the end of the contract year, if at any time the Contractor was assessed for liquidated damages in the prior year, the State may reduce the Contractor's incentives and value-added opportunities award payouts by the prorated amount of months liquidated damages were assessed. For example, if liquidated damages are assessed for two (2) months out of the twelve months, then the incentives and value-added opportunities awards shall be reduced by 1/6 or 16.66%. Any reduction in incentives and value-added opportunities awards payouts shall not exceed the liquidated damages assessed in total for the prior year.

#	Incentive/ Value -Added Opportunity	Incentive/Value-Add Description	Incentive/Value-Add Mechanism	Incentive/Value-Add Frequency	Incentive/Value-Add Revenue
1	Competitions	The Contractor agrees to identify relevant national and/or international competitions and collaborate with IOT to submit Indiana's IN.gov website, applications and services for consideration with the plan of achieving 1st place awards.	The Contractor will receive payment per achievement of a 1st place award.	Up to ten (10) 1st place awards annually	$2,500 per 1st place award
2	System Growth	The Contractor agrees to employ growth strategies to help the State generate additional data management and sales program-related utilization and business	The Contractor will receive payment relative to the increase in data sales revenue from baseline. (Current Revenue – Baseline Revenue) * (Incentive). See example scenario for Years 1-4 of the contract below.	Annually	The Contractor will be paid 10% of the growth in data sales revenue, with previous year's data sales serving as the baseline.
3	Customer Service Scores	The Contractor agrees to exceed the requirements of SLA #13 and achieve at least a 4 out of 5 rating on more than 90% of Project Close-out surveys	The Contractor will receive payment each quarter that SLA #13 is exceeded	Quarterly	$5,000 per quarter that the incentive is met

4	State and Local Migrations	The Contractor agrees to fund growth in software expenses and operating costs as more state and local governments migrate to the IN.gov Program.	The Contractor will receive payment upon successfully pursuing, signing up, and developing new websites for local governments.	Up to 200 new sites annually	$250 per new website

Incentive 2 Example:

Benchmark Revenue	$15,000,000.00
Incentive	10%

	Revenue	**Increase From Benchmark**	**Incentive Payment**
Contract Year 1	$15,500,000.00	$500,000.00	$50,000.00
Contract Year 2	$14,950,000.00	-$50,000.00	$0.00
Contract Year 3	$15,250,000.00	$300,000.00	$30,000.00
Contract Year 4	$16,000,000.00	$750,000.00	$75,000.00

Cost Proposal Narrative

OVERVIEW

Tyler Indiana's pricing reflects our strong desire to deliver on the State's innovative vision and to earn the right to continue to provide award winning digital services to Indiana businesses and citizens. After thorough review of the detailed RPF documents provided, Tyler Indiana fully understands the scope of the services to be provided under baseline services and has priced our response in a way that we are confident in our ability to deliver all required services at the proposed cost. Tyler Indiana understands the scope of work changes from Addendum 3 and our staffing and pricing reflects this new paradigm.

BASELINE SERVICES

ANNUAL BASELINE SERVICES PRICE

All baseline services defined within the RFP have been thoroughly evaluated and priced to fit within the total 4-year proposal price of $22,800,767.00. Based on our expertise in serving the State for the past 28 years, Tyler Indiana is confident that we can continue to deliver cutting-edge services while also meeting the new expectations required under this RFP. The following details our pricing strategy as it pertains to each section of the Technical Proposal.

Program Management - Tyler Indiana has vast experience with building and maintaining a strong and successful program. Our highly experienced management team paired with the support of national departments will ensure each requirement is met or exceeded. As part of our investment in the Minority Business Enterprise (MBE) program, Tyler Indiana has selected a partner who will assist in monitoring our progress and trends against the contract requirements and key performance indicators.

Staffing - Thoroughly analyzing the scope of the RFP and leveraging our vast experience, Tyler Indiana has proposed a team that will be certain to meet the requirements under baseline services and support future growth of the IN.gov Program. Key pieces of the RFP were used to curate the proposed team. For example, changes such as the removal of legacy applications and reclassification of application development to Future Work, required fewer development resources as part of Baseline. Tyler Indiana will leverage Tyler shared resources for Future Work as needed therefore ensuring the Baseline staff are focused on their key objectives under the contract and allowing us to bring a tremendous breadth of skill sets to meet the needs of the State.

Infrastructure Technology - Tyler Indiana has made significant investments over the years to provide an enterprise datacenter capable of meeting the demands of Hoosiers and expectations of the State of Indiana. Our pricing allows us to continue to place a focus on infrastructure technology and provide leading products and services to support the requirements of the RFP.

Project Management - Running an operation as large as IN.gov requires proven processes and tools to effectively manage projects across the enterprise. From managing a major website deployment, to managing a datacenter upgrade, Tyler Indiana's team will have the tools and expertise required to effectively complete work that meets the requirements of the RFP.

Reporting - Our teams are no stranger to effectively and efficiently producing reports that help to validate the health of a program as vast as IN.gov. Staff will be armed with the tools and technologies needed to successfully meet all requirements. Tyler Indiana will also be investing in services from our MBE to provide report development, execution, and oversight to ensure we are consistently evaluating our reporting strategies to validate success and identify improvement opportunities.

Training - Throughout our history, the Tyler Indiana team has trained thousands of state and local government partners. The pricing proposal ensures that we have sufficient staffing and resources to execute a robust training program and include the addition of a Training Specialist through an MBE partner.

Help Desk Customer Support - Ensuring our government partners and residents of the state have memorable help desk and customer support interactions is a priority for Tyler Indiana. The pricing proposal includes not only help desk services and tools necessary to assist IN.gov stakeholders, but it also includes project management oversight to ensure all tickets are logged properly, assigned to the appropriate staff, and status is communicated clearly and regularly to the partners. Tyler Indiana will have the ability to expand customer support capacity at any time to address peak seasons utilizing Tyler's shared customer support team which consists of 40+ Tyler employees located within the United States who meet all the requirements set forth in the procurement. This greatly expands the capacity of the Indiana-based team.

Marketing - Tyler will be providing its national marketing services through the pricing offered under this RFP. The national marketing team are experts in e-government marketing and are tasked with maintaining organizational relationships, developing and executing marketing campaigns, and creating collateral that can be leveraged by the state.

Invoicing - Ensuring our partners and customers receive accurate and detailed invoices is vital to the continued success of IN.gov. Our pricing includes the utilization of our enterprise invoicing and billing system that not only generates transaction level detail reports and invoices, but also manages account receivables on behalf of the state.

Security & Privacy - Tyler Indiana understands the importance of security and privacy and has priced our response to ensure each of the required items are successfully completed. Through investments in tools at the local level to enterprise support from our security experts at a national level, our pricing ensures that Indiana will be supported by these vital resources.

Web Portal - As the largest tangible deliverable of this RFP, investing in the people, tools, and processes to manage the IN.gov Web Portal is critical to overall program success. Our pricing supports a Creative Services team who have over 85 years of combined experience specifically focused on IN.gov. We are confident in our ability to meet and exceed the expectations of this Web Portal deliverables.

Innovation and Trends - In addition to employing experts in the e-government space, our pricing includes the utilization of our national team who brings new ideas from states across the nation and are tasked with ensuring Tyler is continually evaluating upcoming trends and technologies.

Application Management – Ensuring our applications are developed securely, efficiently, and pass all applicable requirements is part of our DNA at Tyler. Our pricing proposal includes all of the requirements defined and is supported by our local and national teams.

Data Management and Sales – Our pricing includes the resources and people required to meet all objectives. Through the utilization of our enterprise billing and invoicing system, built specifically for this exact purpose, the team will be equipped with the best tooling possible for the job.

Quality Assurance – Quality is of upmost importance and is why our pricing includes the experience and tooling required for an effective Quality Assurance program. This includes tools to create and manage test cases that seamlessly map tests to business requirements, to processes developed to elicit acceptance criteria as part of requirements gathering.

Initial Transition – While Tyler Indiana is the incumbent, our approach has been to look at this RFP as a new beginning. We have priced our proposal to include transition items such as the evaluation of many of our existing processes and products to ensure we are providing exactly what the state needs.

End of Contract Turnover – Tyler Indiana's pricing will ensure the successful delivery of all items under this RFP. Therefore, at the end of the contract, we will have all the assets and knowledge necessary to complete a successful turnover.

IN.GOV WEB PORTAL SUPPORT ELEMENTS

Tyler Indiana understands the State's desire to continue to expand by offering new services to its customers under this contract. As such, Tyler Indiana has priced our proposal to include the addition of one new Third-Party Portal Managed Application each year during the contract period. Additionally, Tyler Indiana will support up to 200 new domain names each year. These services are a third-party direct expense, and we are pleased to offer these additional services as part of our Baseline Services Price. Please see Cost Assumptions, Conditions, and Constraints for details pertaining to this commitment.

FUTURE WORK

The ability for Future Work provides a great opportunity for Tyler Indiana to grow its economic impact in the State of Indiana. We realize that Indiana will be trusting us to provide top-notch services under this category and are grateful for the opportunity to provide these services. As such, Tyler Indiana is proposing extremely competitive rates that we hope will earn future business while also ensuring we are able to bring top talent to every engagement we complete on behalf of the IN.gov Program.

POLITICAL SUBDIVISION

BASELINE SERVICES

Serving local government as part of baseline services is included as part of our pricing. This includes ensuring licensing of third-party products supports increased usage, our staffing plan can successfully implement and support growth, all while ensuring each political subdivision receives the same level of service.

ADDITIONAL POLITICAL SUBDIVISION SERVICES

Our pricing approach has considered the ability for political subdivisions to choose billable services that reside outside the scope of the baseline services cost. This has allowed Tyler Indiana to propose a more modest annual increase in baseline services to cover operating cost increases such as staff and third-party software.

ADDITIONAL PRICING

As requested, Tyler Indiana provided insight into the cost of each of the Third-Party Portal Managed services. Our cost proposal included anticipated annual increases in pricing, as well as the addition of a new product being added each year. In the event a third-party dramatically increases their cost for a product, Tyler Indiana will consult with the state and potentially look at alternatives to ensure these costs remain close to our anticipated increases year-over-year.

VALUE ADDED OPPORTUNITIES

Tyler Indiana appreciates the opportunity to provide suggestions for incentives under this opportunity. When successful in expanding the IN.gov Program during the contract period, we anticipate an increase in support and licensing expenses year-over-year. The approach in our response suggests incentives to help support those increases as the program grows over time.

CHAT BOT APPROACH

In the event the state determines that chat bot services are outside the scope of the Contract Scope of Work, Tyler Indiana will reduce the annual Baseline Services cost by $10,000.

Cost Assumptions, Conditions, and Constraints

OVERVIEW

Tyler Indiana is pleased to provide competitive pricing for a program as vast as IN.gov. Our deep experience with providing IN.gov Program services provides us with a unique view on what it takes to effectively operate IN.gov reliably and securely. Due to changes in the RFP compared to current operations, the following assumptions, conditions, and constraints have been considered in our pricing.

STAFFING

1. Due to the impact of Addendum 3 removing all legacy applications from scope, Tyler Indiana has reduced the staffing levels required to complete the work under this RFP. This does not imply Tyler Indiana will be less effective at providing services, rather, it applies our assumption that the Baseline Services under this RFP do not include legacy applications, the addition of new custom applications, and custom application enhancements, including the existing applications listed in Exhibit 1 – Current Application Inventory vF.xlsx.
2. The RFP specifies the maximum number of websites and domains that must be completed as part of Baseline Services. Due to a baseline staffing minimum not being defined, Tyler Indiana assumes it has the right to modify the staffing plan and adjust baseline staffing up or down according to the work available. Tyler Indiana agrees that it must meet the demands of the State in an acceptable manner with an appropriate level of staff and will increase staffing as needed based on the demand of Baseline Services, so long as the demand does not exceed the limits specified in the RFP.

THIRD-PARTY PORTAL MANAGED APPLICATIONS

1. Tyler Indiana is committing to a substantial cost to provide the Third-Party Portal Managed Applications as a part of Baseline Services. In the event a third-party dramatically increases the cost of a service(s), Tyler Indiana assumes it can replace the third-party product with an alternative that is suitable to the State. In the event an alternative is not available, Tyler Indiana assumes the State will be willing to discuss the removal of the product or approve an increase in the Baseline Services amount to help offset the additional costs.
2. In the event that the State requests to increase licensing or usage of a Third-Party Portal Managed Application that results in a significant increase in the annual expense or incurs a large third-party implementation fee, Tyler Indiana assumes it has the ability to consult with the State on the increased costs and provide alternative products or solutions that can offer similar outcomes.
3. The RFP requires Tyler Indiana to agree to a minimum number of new Third-Party Portal Managed Applications each year. Tyler Indiana agrees to provide one new application annually with an annual cost not to exceed $50,000.00. In the event Tyler Indiana is requested to procure a product in excess of $50,000.00 in one-time and/or annual costs, Tyler Indiana assumes the State will increase Baseline Services to cover anything above that amount or allow Tyler Indiana to provide alternative products or services that can offer similar outcomes.

DOMAIN NAMES

1. Tyler Indiana is pleased to provide up to 200 new domain names annually under Baseline Services. Constraints to proving these domain names are (1) it does not include “Premium Domains” that are significantly more expensive than typical domain names and (2) it does not include purchasing domains from private entities who current own a domain. The maximum amount per year for a domain name cannot exceed $30.00 per domain per year.

Contract #XXXXX: IN.gov Web Portal
Exhibit 3
Service Level Agreements (SLAs)

This exhibit reflects the Service Level Agreements (SLAs) to which the State shall hold the Contractor accountable. The Service Level Agreements will have associated liquidated damages for failure to meet the standards. Imposition of liquidated damages is discretionary.

The Contractor shall be responsible for continually monitoring all service levels. The Contractor shall furnish a monthly report detailing their performance against all Service Level Agreements that shall be delivered no later than seven days after the start of the following month. The State will discuss and give the Contractor the opportunity to respond to performance standard issues, and may waive, give the Contractor the opportunity to earn back, or reduce the liquidated damage based on circumstances of a particular performance standard failure.

Liquidated damages will be capped at 10% of the total Baseline Services cost. Damages will be assessed on a monthly basis following receipt of the Contractor's performance report. If it is determined that the Contractor has failed to meet the agreed to service standards, payment will be withheld equal to the liquidated damage percentage at invoice payment.

The State will grant the Contractor the opportunity to earn back the liquidated damage amount. In order to earn back the liquidated damage, the Contractor must meet the metric in the following two reporting periods.

At the end of the contract year, if at any time the Contractor was assessed for liquidated damages in the prior year, the State may reduce the Contractor's incentives and value-added opportunities award payouts by the prorated amount of months liquidated damages were assessed. For example, if liquidated damages are assessed for two (2) months out of the twelve months, then the incentives and value-added opportunities awards shall be reduced by 1/6 or 16.66%. Any reduction in incentives and value-added opportunities awards payouts shall not exceed the liquidated damages assessed in total for the prior year.

An SLA performance review with the State Technology Executive Team shall occur every 6 months. An analysis of the SLAs and Contractor's performance against them will occur between the two parties as needed.

#	SLA	Service Level Agreement Description	Minimum Service Level	Algorithm	Reporting Frequency and Method	Liquidated Damage
1	System Uptime	The Data Center, critical applications to IOT, and the Account Database or System, shall maintain system uptime against a 24-hours per day, 7 days per week operating schedule, excluding maintenance time.	99.9% uptime other than scheduled maintenance time	Monthly calculation of (system uptime for a given month/all time (other than scheduled maintenance) in a given month)	Gathered and reported to the State as part of the Monthly Performance Report	*1.0% of monthly Baseline Costs for the month of the occurrence*
2	IN.gov Performance	The Contractor shall ensure IN.gov webpages maintain a response time of at most one second.	99.99% adherence to the response thresholds, other than during scheduled maintenance	Monthly calculation of system response time that meets the metric/all time (other than scheduled maintenance) in a given month	Gathered and reported to the State as part of the Monthly Performance Report	*1.0% of monthly Baseline Costs for the month of the occurrence*
3	Project Delivery	All discretionary (SOW/TO) work will be completed on time and within budget as set forth in the SOW/TO	A Statement of Work (SOW) / Task Order (TO) will be completed for all discretionary work items in accordance with Scope of Work Sections 1.4.2.2 and 1.4.2.3. Unless a delay is caused by the agency, which is properly documented and mutually agreed upon by IOT, all work efforts of this type will complete within+/- 5% of the timeline and within the budget outlined in the SOW /TO and any associated Change Orders.	To be determined by SOW/TO.	Compiled and analyzed against expected delivery dates and budgets in the Weekly Status Report.	*2.0% of monthly Baseline Costs for the month of the occurrence. The ability to assess liquidated damages will be determined on a per-project basis, and liquidated damages will be included in a SOW/TO at the sole discretion of IOT*

4	Project Quality	All discretionary (SOW/TO) work must be of a consistently high quality.	No changes made to the production portal will need to be backed out or be considered materially non-functional in production as a result of an egregious oversight by the Contractor.	To be determined by SOW/TO.	State shall be notified within 24 hours of any production changes that must be backed out or rereleased within 1 month. Instances shall also be compiled in the Weekly Status Report.	*2.0% of monthly Baseline Costs for the month of the occurrence. The ability to assess liquidated damages will be determined on a per-project basis, and liquidated damages will be included in a SOW/TO at the sole discretion of IOT*
5	Privacy and Security Compliance	**The Contractor shall be compliant with federal laws and regulations, Indiana Law and regulations, and standards outlined in Scope of Work Section 1.11.**	100% compliance with all applicable federal laws and regulations, Indiana Law and regulations, and standards outlined in Scope of Work Section 1.11.	Any applicable incidents of non-compliance discovered by or reported to the State shall be cured by the Contractor within 30 calendar days upon notice by the State. (Repeated failures to cure would be cause for termination of the agreement.)	On an incident-by-incident basis	*2.0% of monthly Baseline Costs for the month of the occurrence*

6	Intrusion and Data Breaches	**For confirmed data breaches and intrusions of information subject to IC § 24-4.9 the Contractor shall provide as much detail as is available at the time about the nature of any intrusion and shall advise the State of all actions taken to mitigate.**	For 100% of data breaches and intrusions, a report with as much detail and information as is available at the time shall be delivered within 12 hours to IOT.	Calculation per incident: time of data breach/intrusion to time of report submittal.	On an incident-by-incident basis	*1.0% of monthly Baseline Costs for the month of the occurrence will be delivered to IOT*
7	Disclosure of a Security Breach Protocol	**If a security breach occurs and involves information subject to IC § 24-4.9 in the possession of the Contractor, the Contractor shall fully comply with the notification and reporting requirements of Indiana Code § 24-4.9.**	100% compliance with the protocol of Indiana Code § 24-4.9. and Scope of Work Section 1.11.12.	If breach were to occur, documentation proving Contractor followed Indiana Code § 24-4.9. and Scope of Work Section 1.11.12.	On an incident-by-incident basis	*1.0% of monthly Baseline Costs for the month of the occurrence*

8	System Recover-ability	The Contractor shall report all instances of non-availability or non-reliability of static content, critical applications to IOT, and the Account Database or System within the expected service levels listed to the right.	A) Any outage must be reported to the State within 1 hour of knowledge of the outage. B) An initial outage report must be submitted to IOT within 24 hours of the incident. C) A detailed incident report must be submitted to IOT within three (3) business days of the incident. D) All static content and services deemed critical (including all revenue-generating services and (iii) all services provided to the Governor's Office, LSA, ISP, DHS, DOR, BMV, SOS and PLA) will be fully recovered and available to portal users and administrators with 4 hours. E) Non-critical content and systems will be recovered within 72 hours.	All outages will be reported regardless of root cause.	On an outage-by-outage basis and also compiled in the Weekly Project Status Report.	*N/A*
9	Team Stability	To provide consistent service to the state, the Contractor must provide a stable, dependable team structure.	Team attrition of no more than 8% per 6-month reporting period is expected.	For each 6-month reporting period, attrition shall be calculated as follows: $\frac{\text{(Team members who departed during the reporting period)}}{\text{((team size at the beginning of the period) + (team size at end of period)/2).}}$ *For the purposes of this SLA, team size will be a count of all team members in a full-time role (>30 weekly expected hours) expected to complete at least 500 hours of work.*	Team Stability data will be compiled and reported to the State every 6 months in a stand-alone deliverable.	*N/A*

10	Background Checks	Starting from the day one of the contract and continuing until the contract is no longer in effect, all employees must have undergone a fingerprint based criminal history check within 60 days of being assigned to this account.	100% compliance for all Contractor and subcontractor personnel	Calculation: Date contract starts compared to date fingerprints required to complete the criminal history record background check are submitted	Reported via a standalone deliverable within two weeks after the 90th day of the contract	*N/A*
11	Staff Removal	If the State becomes reasonably dissatisfied with the work product of or the working relationship with an individual assigned to work on this Contract, the Contractor must either replace or reassign such individual.	100% compliance with removing or reassigning Contractor or subcontractor employees found unacceptable to the State within two (2) weeks of the request for removal, or sooner if requested by the State.	Calculation per incident: date of request compared to date of removal / reassignment.	On an incident-by-incident basis and reported to the State as part of the Monthly Performance Report.	*N/A*

1 2	Web Portal Support Elements	The Contractor shall uphold their commitments to the baseline included quantities stated in their RFP Cost Proposal for the following support elements as part of Baseline Services: i. The addition of websites to include state and local government agencies. ii. The addition of new third-party applications iii. The addition of domain names	Each year, the Contractor shall accommodate 100% of support element requests up to the addition of two hundred (200) domain names and the addition of one (1) new third-party portal managed application, as stated in the Contractor's RFP Cost Proposal and reflected in Contract Exhibit 2, as part of Baseline Services.	Yearly calculation of support element requests compared to the (200) domain names and (1) new third-party portal managed application stated in the Contractor's RFP Cost Proposal and reflected in Contract Exhibit 2.	Reported via a standalone deliverable within one month after the end of each contract year.	*N/A*

13	Project Close-out Surveys	The Contractor will institute a structured method to actively solicit direct customer satisfaction feedback (including citizens, businesses, and agencies). When discretionary work (SOW/TO) is completed, the Contractor must send out a project close out survey to the client and submit the results of the survey to the State.	The Contractor shall achieve a 4 or 5 out of 5 rating on 90% of surveys.	Takes total responses with a 5 and 4 divided by total number of responses.	Close-out survey results will be gathered, analyzed against historical trends, and reported to the State at least every 6 months in a stand-alone deliverable.	*N/A*
14	Support Request Responsiveness	The Contractor shall respond to all requests for support in a timely manner. This includes but is not limited to phone calls sent to help desk queues, and online chats.	Acceptable timeframe for an initial non-automated response to all support inquiries for each available channel are: • Phone Calls (during support hours): All calls answered within 4 minutes • Emails (during support hours): Email replies acknowledging the request within .5 working day • Online Chat: All chat requests acknowledged within 4 minutes	Details for each support category will be tracked and reported. All calls shall be logged with start and end time. All emails shall be logged with a received and acknowledged time. All chat requests shall be logged with a received and acknowledged time. All elements should be measured against the required timeframes.	Support Request Responsiveness data will be gathered, analyzed against historical trends, and reported to the State at least every 6 months in a stand-alone deliverable.	*N/A*

15	Reporting Timeliness	**The Contractor shall produce all reports outlined in Scope of Work Section 1.5 in accordance with timeframes outlined in the Contract.**	100% of reports meet the required timeframes outlined in the Contract.	Monthly aggregation of all reports submitted and measured against required timeframes.	Reported to the State as part of the Monthly Performance Report	*N/A*
16	Reporting Accuracy	**The Contractor shall produce all reports outlined in Scope of Work Section 1.5 accurately in accordance with requirements.**	100% of reports are delivered accurately in accordance with requirements.	Monthly aggregation of all reports submitted and measured against Contract requirements.	Reported to the State as part of the Monthly Performance Report.	*N/A*
17	Content Change Priority Level	**The Contractor shall meet the priority level change timeframes listed in Scope of Work Section 1.12.5.**	100% compliance for all content changes defined as high priority. 99% compliance for all content changes defined as medium or low priority.	Calculation per incident: date of request compared to date of content change.	On an incident-by-incident basis and reported to the State as part of the Monthly Performance Report.	*N/A*

State of Indiana Additional Terms and Conditions
Software as a Service Engagements

Exhibit 4 to the Contract between the State acting through the Indiana Office of Technology and the Contractor.

DEFINITIONS

Data means all information, whether in oral, written, or electronic form, created by or in any way originating with the State, and all information that is the output of any computer processing, or other electronic manipulation, of any information that was created by or that in any way originated with the State, in the course of using and configuring the Services.

Data Breach means any actual or reasonably suspected unauthorized access to or acquisition of Encrypted Data.

Encrypted Data means Data that that is required to be encrypted under the contract and Statement of Work.

Indiana Office of Technology means the agency established by Ind. Code § 4-13.1-2-1.

Information Security Framework means the State of Indiana's written policy and standards document governing matters affecting security and available at https://www.in.gov/iot/security/information-security-framework2/.

Security Incident means any actual or reasonably suspected unauthorized access to the contractor's system, regardless of whether contractor is aware of a Data Breach. A Security Incident may or may not become a Data Breach.

Service(s) means that which is provided to the State by contractor pursuant to this contract and the contractors obligations under the contract.

Service Level Agreement means a written agreement between both the State and the contractor that is subject to the terms and conditions of this contract. Service Level Agreements should include: (1) the technical service level performance promises (i.e. metrics for performance and intervals for measure); (2) description of service quality; (3) identification of roles and responsibilities; (4) remedies, such as credits; and (5) an explanation of how remedies or credits are calculated and issued.

Statement of Work means the written agreement between both the State and contractor attached to and incorporated into this contract.

TERMS

1. Data Ownership: The State owns all rights, title, and interest in the Data. The contractor shall not access State user accounts or Data, except: (1) in the normal course of data center operations; (2) in response to Service or technical issues; (3) as required by the express terms of this contract, applicable Statement of Work, or applicable Service Level Agreement; or (4) at the State's written request.

Contractor shall not collect, access, or use Data except as strictly necessary to provide Service to the State. No information regarding State's use of the Service may be disclosed, provided, rented, or sold to any third party for any reason unless required by law or regulation or by an order of a court of competent jurisdiction. This obligation shall survive and extend beyond the term of this contract.

2. Data Protection: Protection of personal privacy and Data shall be an integral part of the business activities of the contractor to ensure there is no inappropriate or unauthorized use of Data at any time. To this end, the contractor shall safeguard the confidentiality, integrity, and availability of Data and shall comply with the following conditions:

a. The contractor shall implement and maintain appropriate administrative, technical, and organizational security measures to safeguard against unauthorized access, disclosure, or theft of Data. Contractor shall implement and maintain heightened security measures with respect to Encrypted Data. Such security measures shall be in accordance with Indiana Office of Technology practice and recognized industry practice, including but not limited to the following:

1. Information Security Framework; and

2. Indiana Office of Technology Cloud Product and Service Agreements, Standard ID: IOT-CS-SEC-010.

b. All Encrypted Data shall be subject to controlled access. Any stipulation of responsibilities shall be included in the Statement of Work and will identify specific roles and responsibilities.

c. The contractor shall encrypt all Data at rest and in transit. The State may, in the Statement of Work, identify Data it deems as that which may be publicly disclosed that is not subject to encryption. Data so designated may be maintained without encryption at rest and in transit. The level of protection and encryption for all Encrypted Data shall meet or exceed that required in the Information Security Framework.

d. At no time shall any Data or processes — that either belong to or are intended for the use of State — be copied, disclosed, or retained by the contractor or any party related to the contractor for subsequent use in any transaction that does not include the State.

e. The contractor shall not use any information collected in connection with the Services for any purpose other than fulfilling its obligations under the contract.

3. Data Location: Storage of Data at rest shall be located solely in data centers in the United States and the contractor shall provide its Services to the State and its end users solely from locations in the United States. The contractor shall not store Data on portable devices, including personal laptop and desktop computers. The contractor shall access Data remotely only as required to provide technical support. The

contractor shall provide technical user support on a 24/7 basis unless specified otherwise in the Service Level Agreement.

4. Notice Regarding Security Incident or Data Breach:

a. Incident Response: contractor may need to communicate with outside parties regarding a Security Incident, which may include contacting law enforcement, fielding media inquiries, and seeking external expertise as mutually agreed upon, defined by law, or contained in the contract. Discussing Security Incidents and Data Breaches with the State must be handled on an urgent basis, as part of contractor's communication and mitigation processes as mutually agreed upon in the Service Level Agreement, contained in the contract, and in accordance with IC 4-1-11 and IC 24-4.9 as they may apply.

b. Security Incident Reporting Requirements: The contractor shall report a Security Incident to the State-identified contact(s) as soon as possible by telephone and email, but in no case later than two (2) days after the Security Incident occurs. Notice requirements may be clarified in the Service Level Agreement and shall be construed in accordance with IC 4-1-11 and IC 24-4.9 as they may apply.

c. Data Breach Reporting Requirements: If a Data Breach occurs, the contractor shall do the following in accordance with IC 4-1-11 and IC 24-4.9 as they may apply: (1) as soon as possible notify the State-identified contact(s) by telephone and email, but in no case later than two (2) days after the Data Breach occurs unless a shorter notice period is required by applicable law; and (2) take commercially-reasonable measures to address the Data Breach in a timely manner. Notice requirements may be clarified in the Service Level Agreement. If the Data involved in the Data Breach involves protected health information, personally identifying information, social security numbers, or otherwise confidential information, other sections of this contract may apply. The requirements discussed in those sections must be met in addition to the requirements of this section.

5. Responsibilities Regarding Data Breach: This section applies when a Data Breach occurs with respect to Encrypted Data within the possession or control of the contractor.

a. The contractor shall: (1) cooperate with the State as reasonably requested by the State to investigate and resolve the Data Breach; (2) promptly implement necessary remedial measures, if necessary; and (3) document and provide to the State responsive actions taken related to the Data Breach, including any post-incident review of events and actions taken to make changes in business practices in providing the Services, if necessary.

b. Unless stipulated otherwise in the Statement of Work, if a Data Breach is a result of the contractor's breach of its contractual obligation to encrypt Data or otherwise prevent its release as reasonably determined by the State, the contractor shall bear the costs associated with: (1) the investigation and resolution of the Data Breach; (2) notifications to individuals, regulators, or others required by federal and/or state law, or as otherwise agreed to in the Statement of Work; (3) a credit monitoring service required by federal and/or state law, or as otherwise agreed to in the Statement of Work; (4) a website or a toll-free number and call center for affected individuals required by federal and/or state law — all of which shall not amount to less than the average per-record per-person cost calculated for data breaches in the United States (in, for example, the most recent Cost of Data Breach Study: Global Analysis published by the Ponemon Institute at the time of the Data Breach); and (5) complete all

corrective actions as reasonably determined by contractor based on root cause and on advice received from the Indiana Office of Technology. If the Data involved in the Data Breach involves protected health information, personally identifying information, social security numbers, or otherwise confidential information, other sections of this contract may apply. The requirements discussed in those sections must be met in addition to the requirements of this section.

6. Notification of Legal Requests: If the contractor is requested or required by deposition or written questions, interrogatories, requests for production of documents, subpoena, investigative demand or similar process to disclose any Data, the contractor will provide prompt written notice to the State and will cooperate with the State's efforts to obtain an appropriate protective order or other reasonable assurance that such Data will be accorded confidential treatment that the State may deem necessary.

7. Termination and Suspension of Service:

a. In the event of a termination of the contract, the contractor shall implement an orderly return of Data in a mutually agreeable and readable format. The contractor shall provide to the State any information that may be required to determine relationships between data rows or columns. It shall do so at a time agreed to by the parties or shall allow the State to extract its Data. Upon confirmation from the State, the contractor shall securely dispose of the Data.

b. During any period of Service suspension, the contractor shall not take any action that results in the erasure of Data or otherwise dispose of any of the Data.

c. In the event of termination of any Services or contract in its entirety, the contractor shall not take any action that results in the erasure of Data until such time as the State provides notice to contractor of confirmation of successful transmission of all Data to the State or to the State's chosen vendor.

During this period, the contractor shall make reasonable efforts to facilitate the successful transmission of Data. The contractor shall be reimbursed for all phase-out costs (i.e., costs incurred within the agreed period after contract expiration or termination that result from the transfer of Data or other information to the State). A reimbursement rate shall be agreed upon by the parties during contract negotiation and shall be memorialized in the Statement of Work. After such period, the contractor shall have no obligation to maintain or provide any Data and shall thereafter, unless legally prohibited, delete all Data in its systems or otherwise in its possession or under its control. The State shall be entitled to any post-termination assistance generally made available with respect to the Services, unless a unique data retrieval arrangement has been established as part of a Service Level Agreement.

d. Upon termination of the Services or the contract in its entirety, contractor shall, within 30 days of receipt of the State's notice given in 7(c) above, securely dispose of all Data in all of its forms, including but not limited to, CD/DVD, backup tape, and paper. Data shall be permanently deleted and shall not be recoverable, according to National Institute of Standards and Technology (NIST)-approved methods. Certificates of destruction shall be provided to the State upon completion.

8. Background Checks: The contractor shall conduct a Federal Bureau of Investigation Identity History Summary Check for each employee involved in provision of Services: (1) upon commencement of the contract; (2) prior to hiring a new employee; and (3) for any employee upon the request of the State. The contractor shall not utilize any staff, including subcontractors, to fulfill the obligations of the

contract who have been convicted of any crime of dishonesty, including but not limited to criminal fraud, or otherwise convicted of any felony or misdemeanor offense for which incarceration for up to one (1) year is an authorized penalty. The contractor shall promote and maintain an awareness of the importance of securing the State's information among the contractor's employees, subcontractors, and agents. If any individual providing Services under the contract is not acceptable to the State, in its sole opinion, as a result of the background or criminal history investigation, the State, in its sole option shall have the right to either: (1) request immediate replacement of the individual; or (2) immediately terminate the contract, related Statement of Work, and related Service Level Agreement.

9. Access to Security Logs and Reports: The contractor shall provide to the State reports on a schedule and in a format specified in the Service Level Agreement as agreed to by both the contractor and the State. Reports shall include latency statistics, user access, user access IP address, user access history, and security logs for all Data. The State's audit requirements shall, if applicable, be defined in the Statement of Work.

10. Contract Audit: The contractor shall allow the State to audit conformance to the contract terms. The State may perform this audit or contract with a third party at its discretion and at the State's expense.

11. Data Center Audit [Modified]: The contractor shall perform an annual independent audit of its data center(s) where Data, State applications, or other State information is maintained. The contractor shall perform this independent audit at its expense and shall, upon completion, provide an unredacted version of the complete audit report to the State. (The contractor may redact its proprietary information from the unredacted version, however.) A Service Organization Control (SOC) 2 audit report or equivalent approved by the Indiana Office of Technology sets the minimum level of a third-party audit.

The State may perform an annual audit of contractor's data center(s) where Data, State applications, or other State information is maintained. The audit may take place onsite or remotely, at the State's discretion. The State shall provide to contractor thirty (30) days' advance notice prior to the audit. The contractor will make reasonable efforts to facilitate the audit and will make available to the State members of its staff during the audit. The State may contract with a third party to conduct the audit at its discretion and at the State's expense. If the contractor maintains Data, State applications, or other State information at multiple data centers, the State may perform an annual audit of each data center.

The parties agree that any documents provided to the State under this paragraph shall be deemed a trade secret of contractor and is deemed administrative or technical information that would jeopardize a record keeping or security system, and shall be exempt from disclosure under the Indiana Access to Public Records Act, IC 5-14-3.

Notwithstanding anything to contrary, Contractor will have at least 15 business days to review potential findings and provide additional clarifications, correct inaccurate information and refute false positives in the security assessment report, and under no circumstances will vulnerability scans or controlled penetration tests be conducted on production environments.

12. Change Control and Advance Notice: The contractor shall give notice to the State for change management requests. Contractor shall provide notice to the State regarding change management

requests that do not constitute an emergency change management request at least two (2) weeks in advance of implementation. Contractor shall provide notice to the State regarding emergency change management requests no more than twenty-four (24) hours after implementation.

Contractor shall make updates and upgrades available to the State at no additional cost when contractor makes such updates and upgrades generally available to its users. No update, upgrade, or other change to the Service may decrease the Service's functionality, adversely affect State's use of or access to the Service, or increase the cost of the Service to the State.

13. Security: The contractor shall, on an annual basis, disclose its non-proprietary system security plans or security processes and technical limitations to the State such that adequate protection and flexibility can be attained between the State and the contractor. For example: virus checking and port sniffing. The State and the contractor shall share information sufficient to understand each other's roles and responsibilities. The contractor shall take into consideration feedback from the Indiana Office of Technology with respect to the contractor's system security plans.

The parties agree that any documents provided to the State under this paragraph shall be deemed a trade secret of contractor and is deemed administrative or technical information that would jeopardize a record keeping or security system, and shall be exempt from disclosure under the Indiana Access to Public Records Act, IC 5-14-3.

14. Non-disclosure and Separation of Duties: The contractor shall enforce role-based access control, separation of job duties, require commercially-reasonable nondisclosure agreements, and limit staff knowledge of Data to that which is absolutely necessary to perform job duties. The contractor shall annually provide to the State a list of individuals that have access to the Data and/or the ability to service the systems that maintain the Data.

15. Import and Export of Data: The State shall have the ability to import or export Data in piecemeal or in entirety at its discretion, with reasonable assistance provided by the contractor, at any time during the term of contract. This includes the ability for the State to import or export Data to/from other parties at the State's sole discretion. Contractor shall specify in the Statement of Work if the State is required to provide its' own tools for this purpose, including the optional purchase of contractor's tools if contractor's applications are not able to provide this functionality directly.

16. Responsibilities and Uptime Guarantee: The contractor shall be responsible for the acquisition and operation of all hardware, software, and network support related to the Services being provided. The technical and professional activities required for establishing, managing, and maintaining the environments are the responsibilities of the contractor. Subject to the Service Level Agreement, the Services shall be available to the State at all times. The contractor shall allow the State to access and use the Service to perform synthetic transaction performance testing.

The contractor shall investigate and provide to the State a detailed incident report regarding any unplanned Service interruptions or outages. The State may terminate the contract for cause if, at its sole discretion, it determines that the frequency of contractor-preventable outages is sufficient to warrant termination.

17. Subcontractor Disclosure: Contractor shall identify all of its strategic business partners related to Services, 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 contractor, and who may be involved in any application development and/or operations.

The contractor shall be responsible for the acts and omissions of its subcontractors, strategic business partners, or other entities or individuals who provide or are involved in the provision of Services.

18. Business Continuity and Disaster Recovery: The State's recovery time objective shall be defined in the Service Level Agreement. The contractor shall ensure that the State's recovery time objective has been met and tested as detailed in the Service Level Agreement. The contractor shall annually provide to the State a business continuity and disaster recovery plan which details how the State's recovery time objective has been met and tested. The parties agree that any documents provided to the State under this paragraph shall be deemed administrative or technical information that would jeopardize a record keeping or security system, and shall be exempt from disclosure under the Indiana Access to Public Records Act, IC 5-14-3. The contractor shall work with the State to perform an annual disaster recovery test and take action to correct any issues detected during the test in a time frame mutually agreed upon between the contractor and the State in the Service Level Agreement.

The State's Data shall be maintained in accordance with the applicable State records retention requirement, as determined by the State. The contractor shall annually provide to the State a resource utilization assessment detailing the Data maintained by the contractor. This report shall include the volume of Data, the file formats, and other content classifications as determined by the State.

19. Compliance with Accessibility Standards: The contractor shall comply with and adhere to Accessibility Standards of Section 508 Amendment to the Rehabilitation Act of 1973, or any other state laws or administrative regulations identified by the State.

20. State Additional Terms and Conditions Revision Declaration: The clauses in this Exhibit have not been altered, modified, changed, or deleted in any way except for the following clauses which are named below:_____

11. Data Center Audit [Modified]

Contract # 00000000000000000000079743
IN.gov Web Portal
Exhibit 5- Implementation Plan

[redacted]

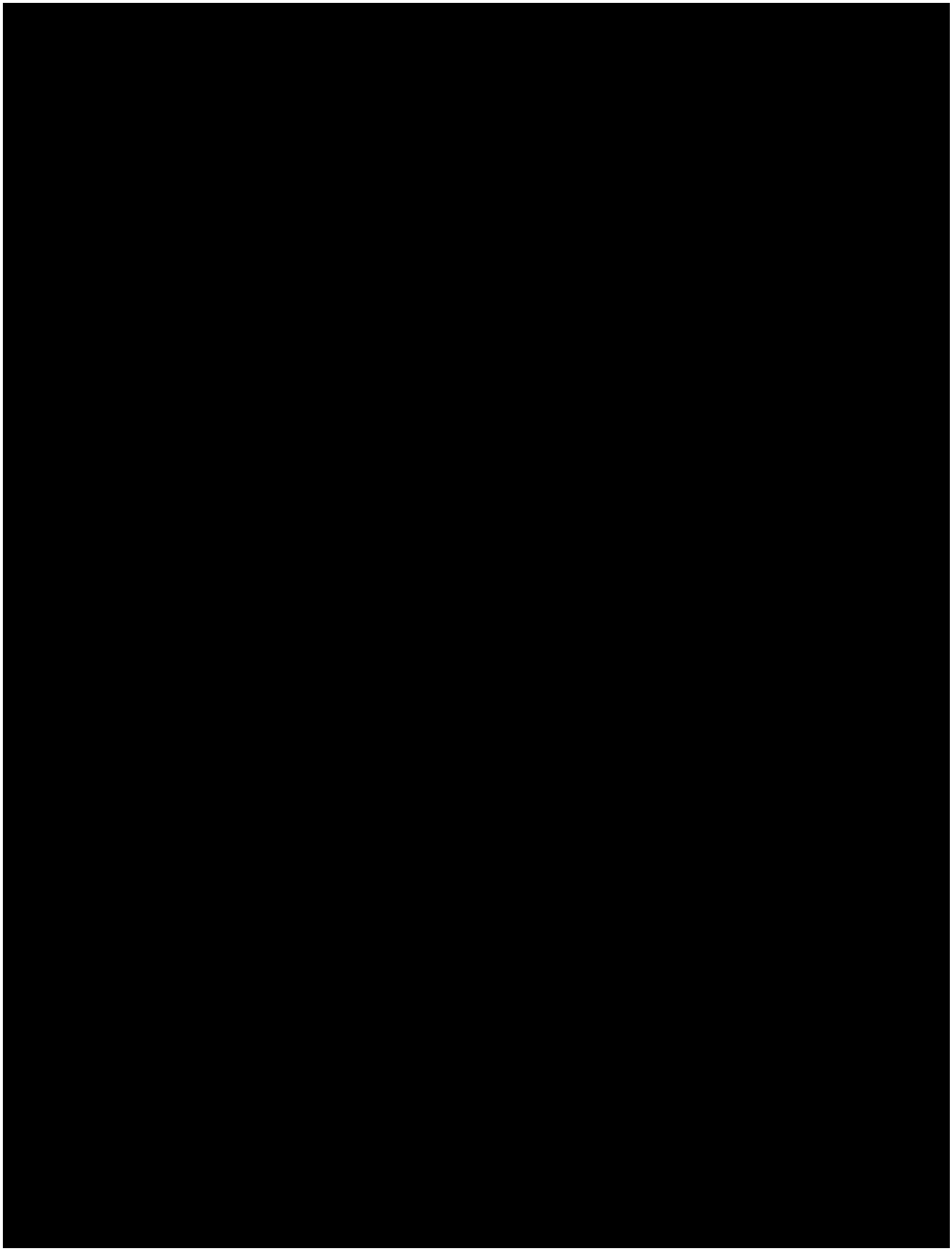
Contract # 0000000000000000000079743
IN.gov Web Portal
Exhibit 6- Innovation Plan

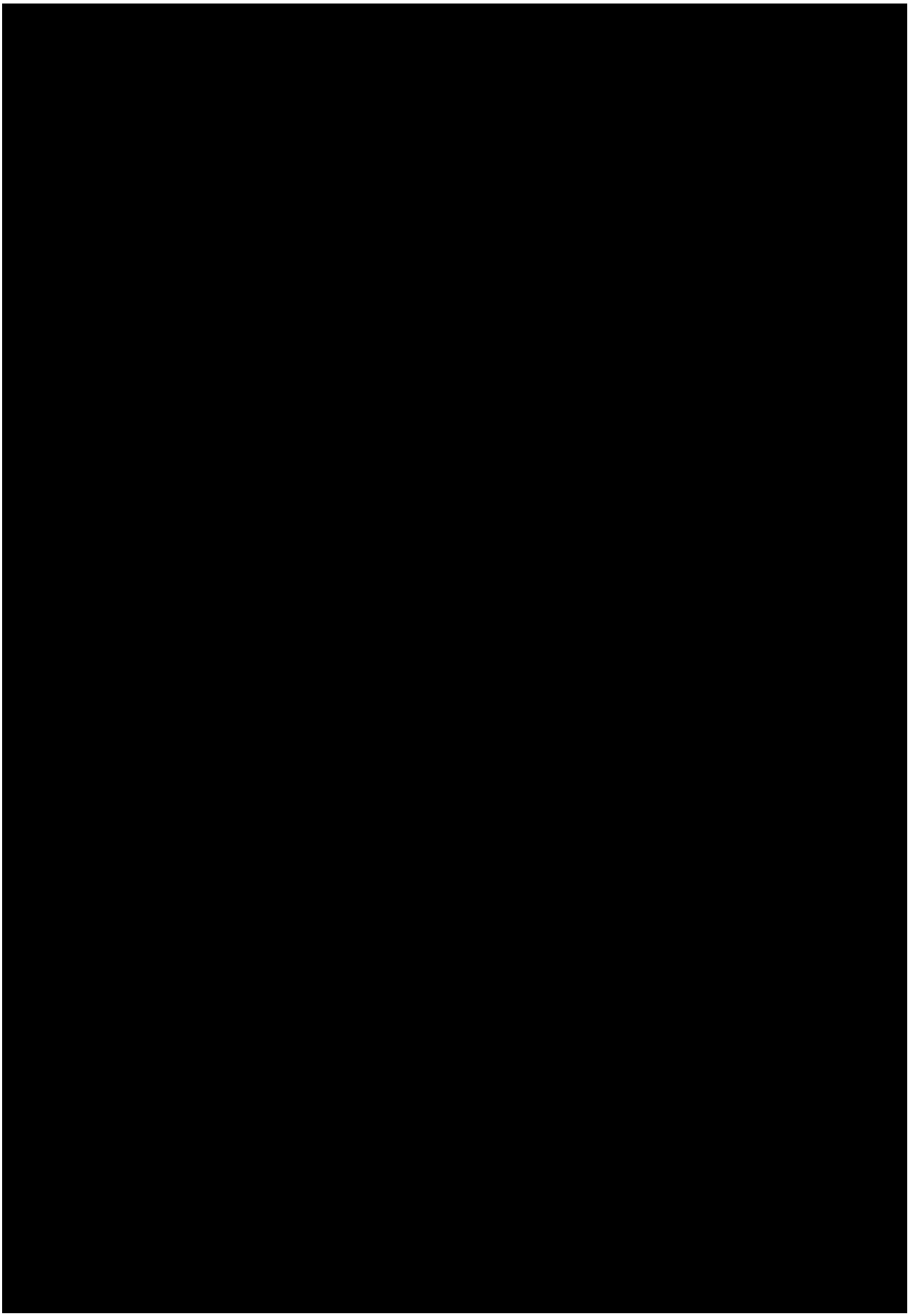
[redacted]

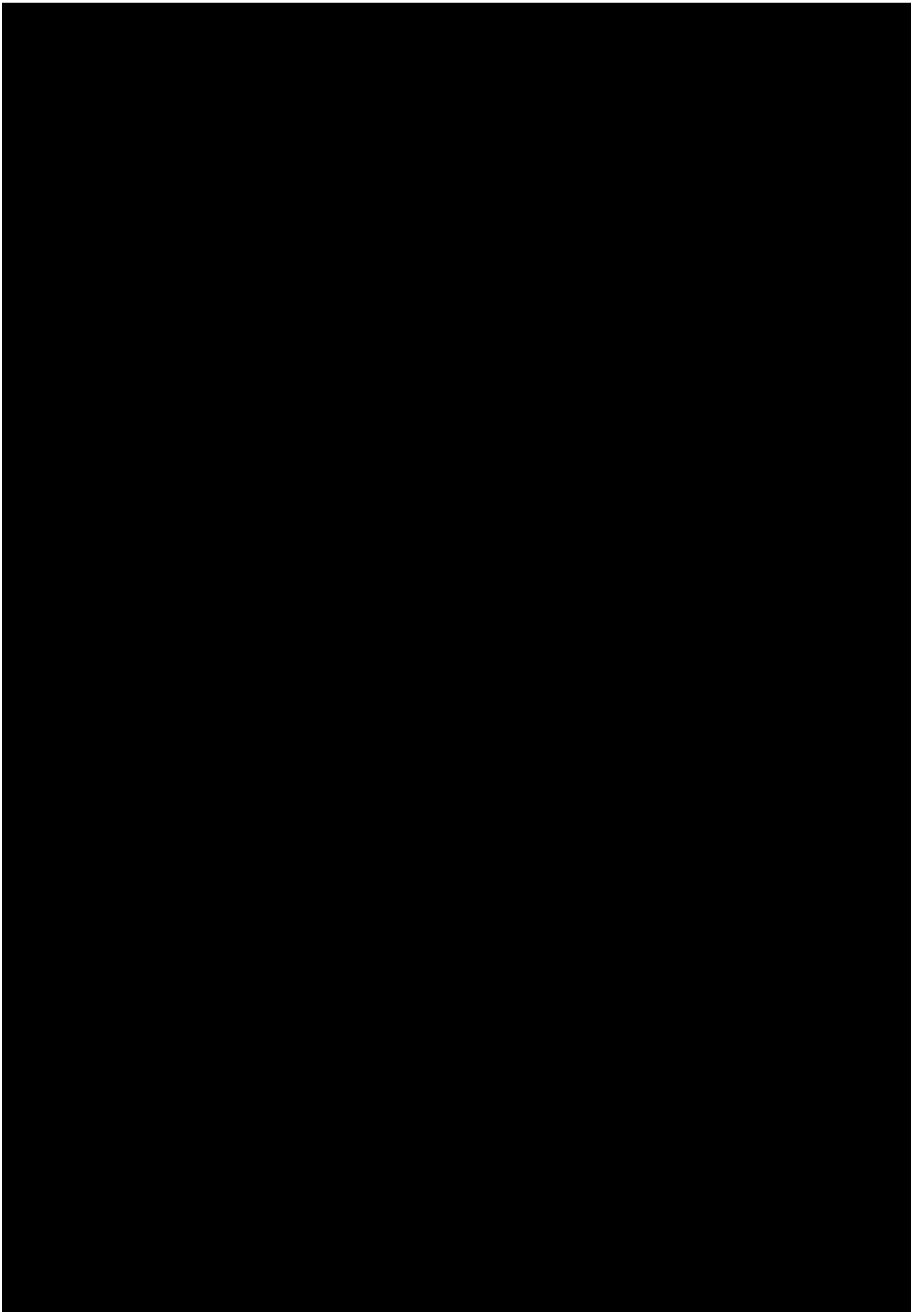
Exhibit 7

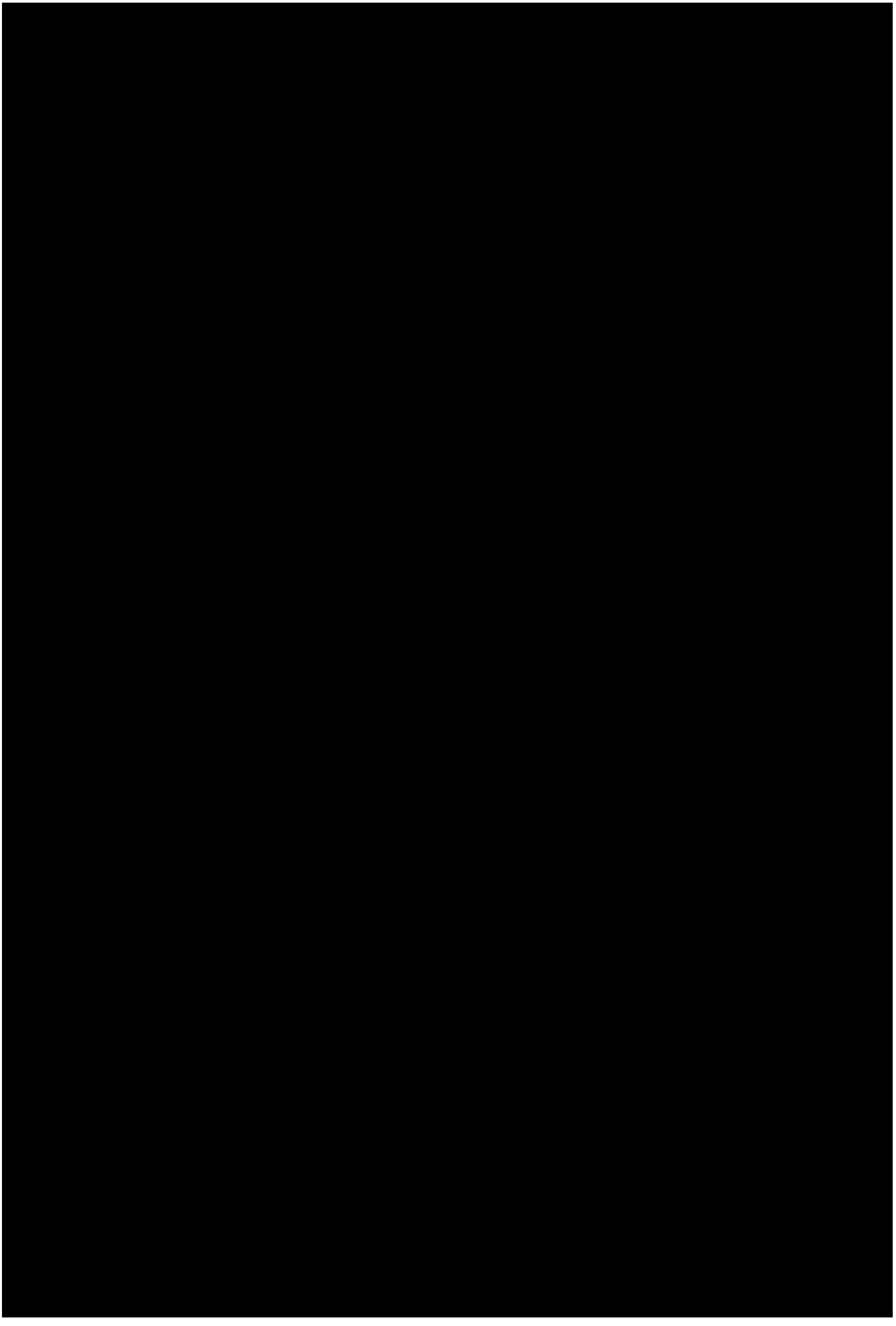
DISASTER RECOVERY PLAN

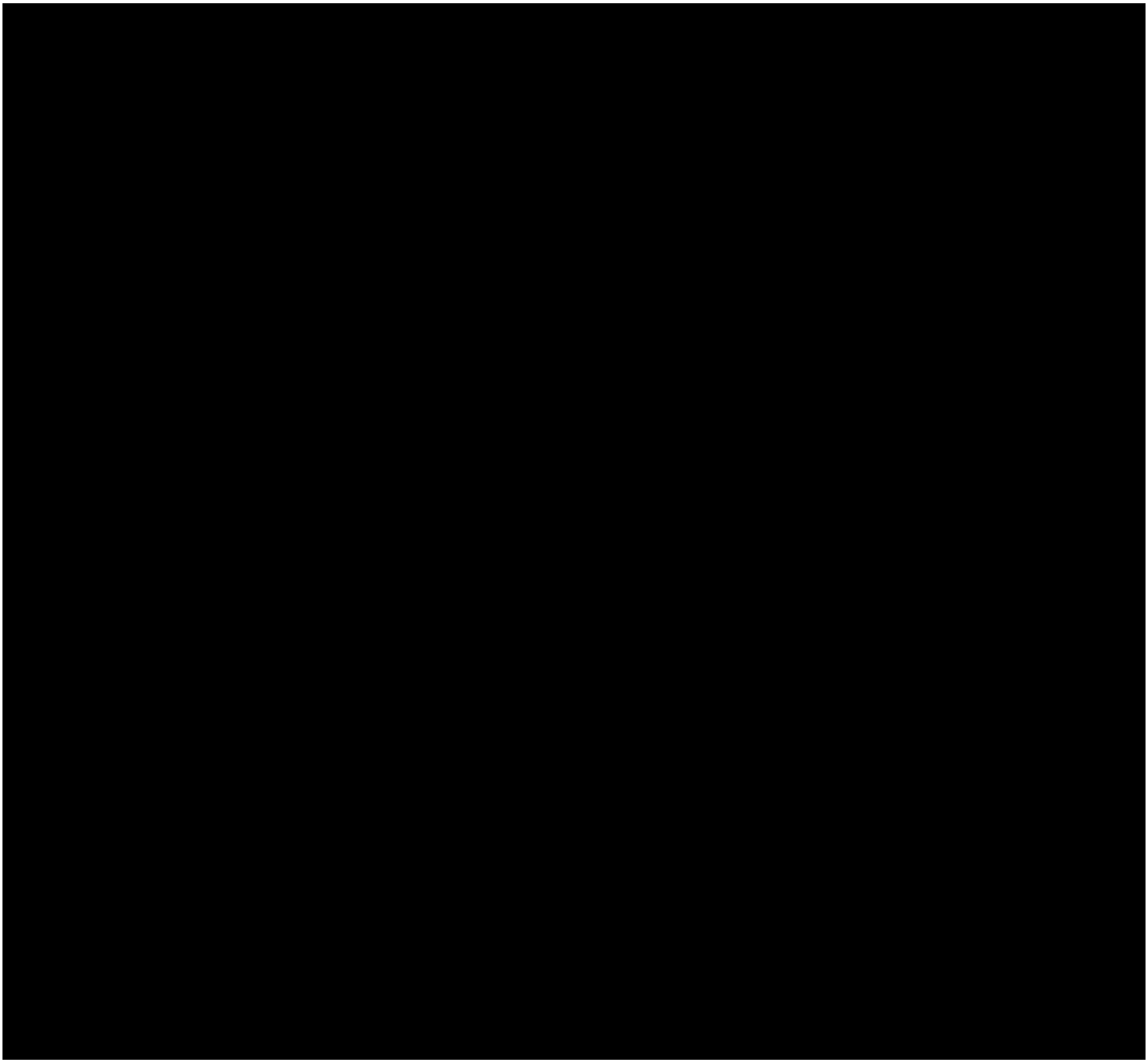
Tyler Indiana Network Operations

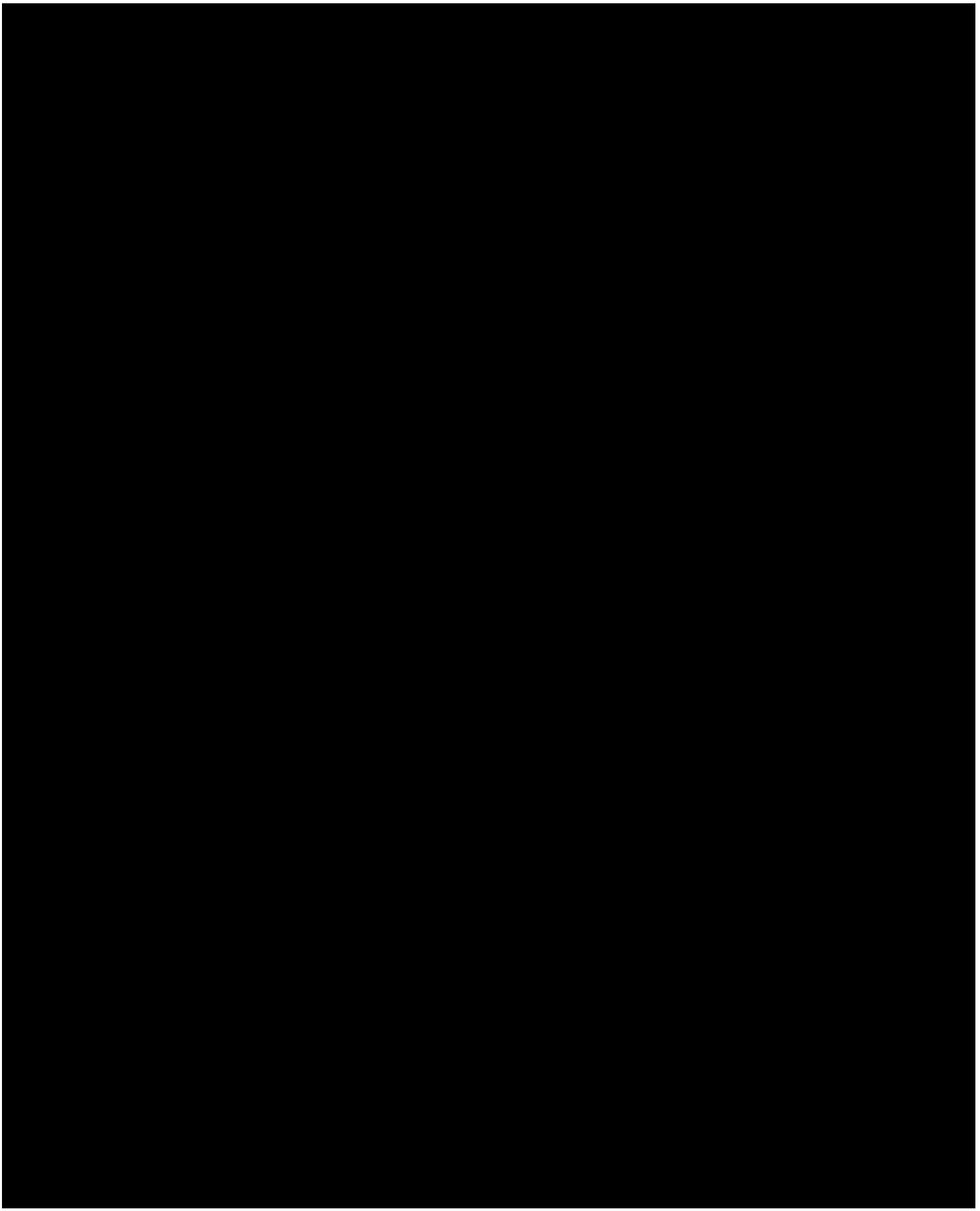


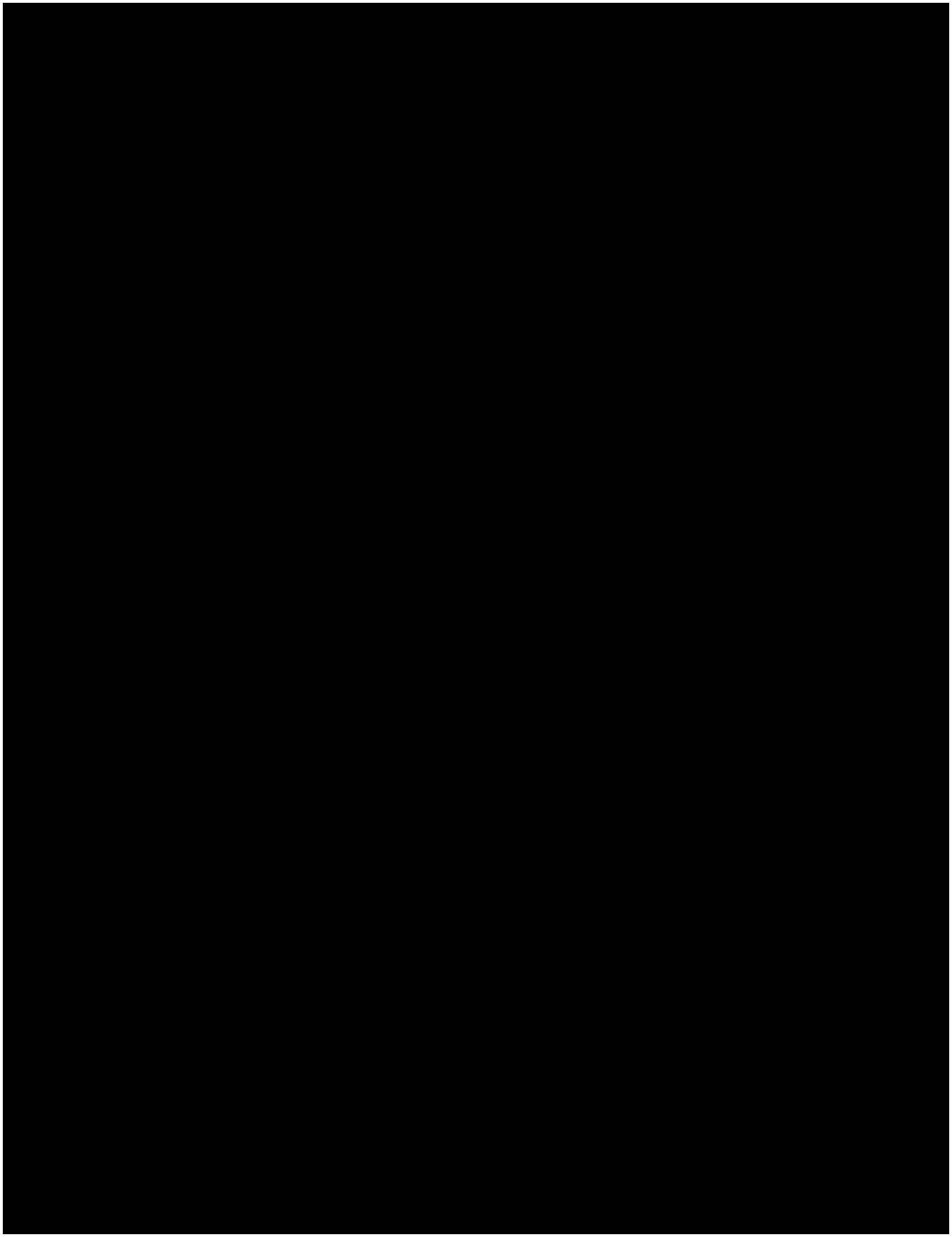


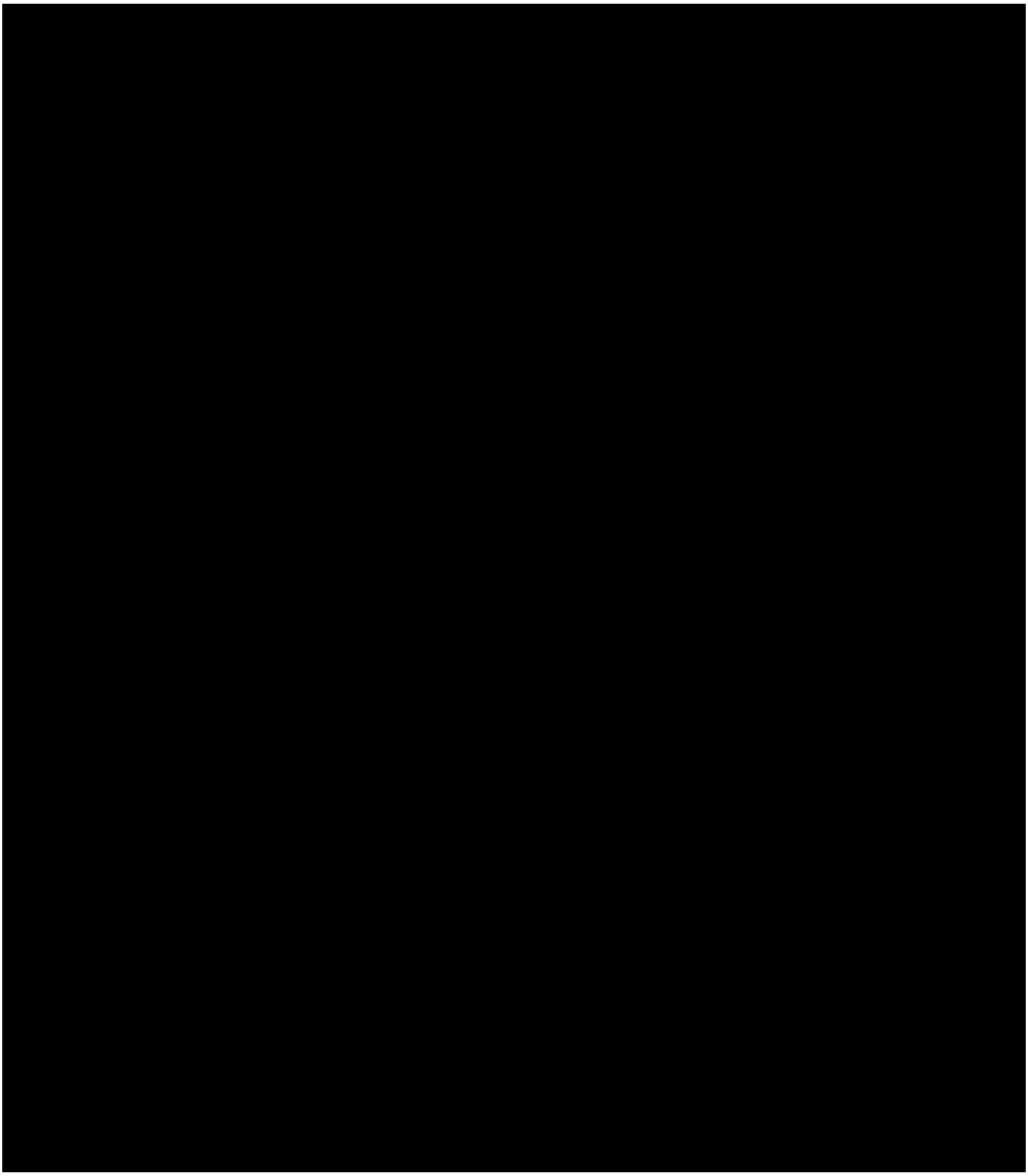


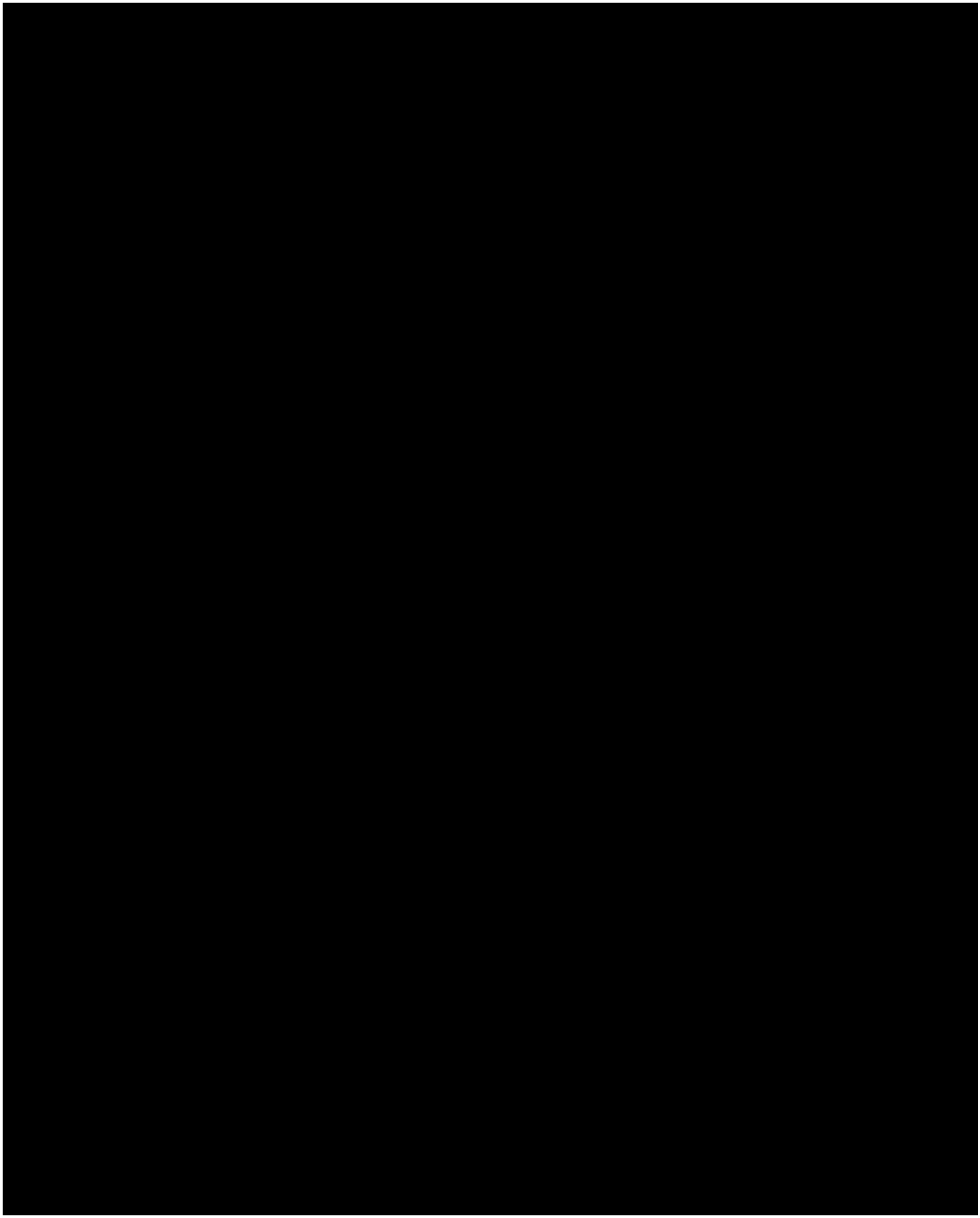


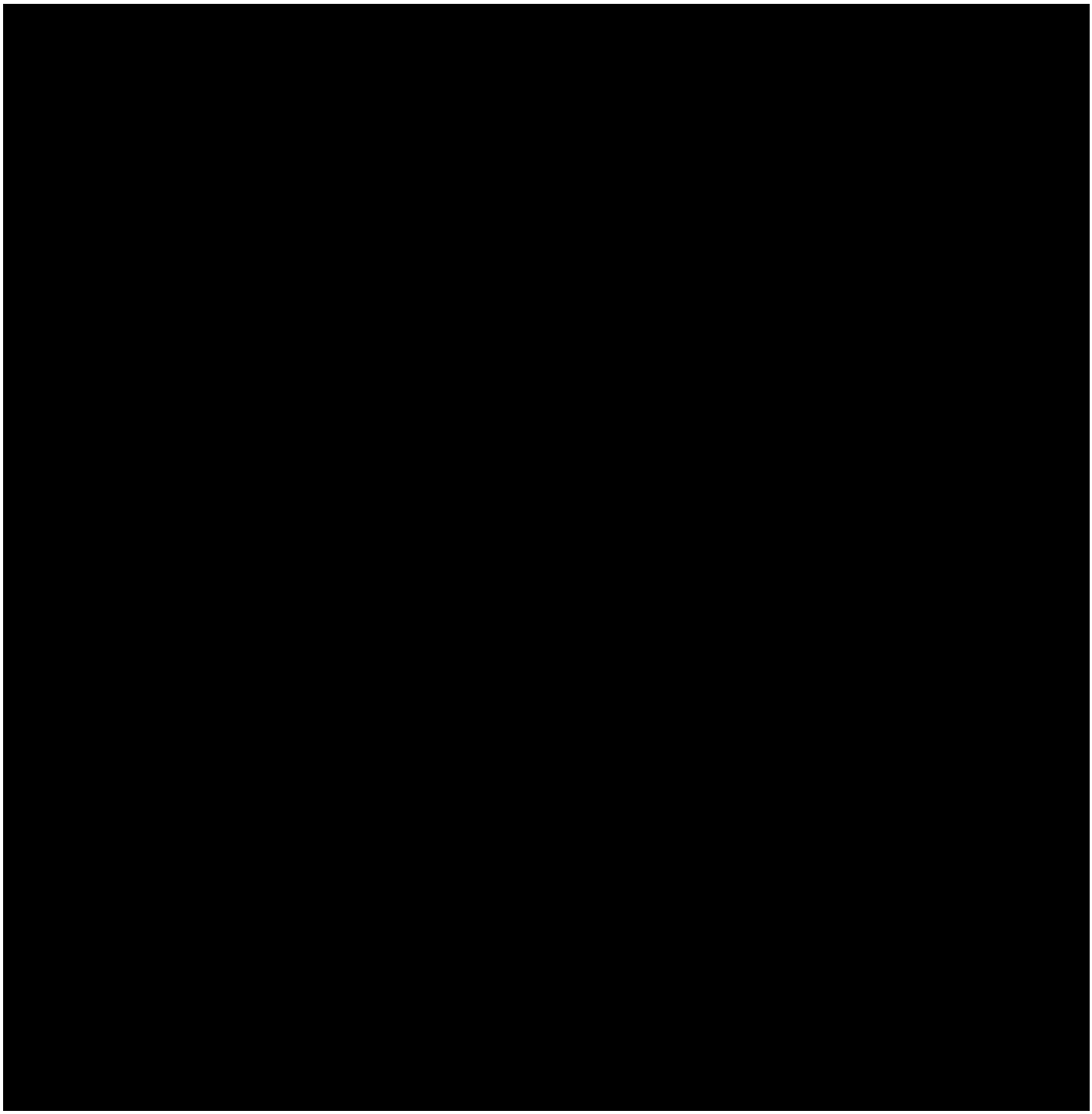


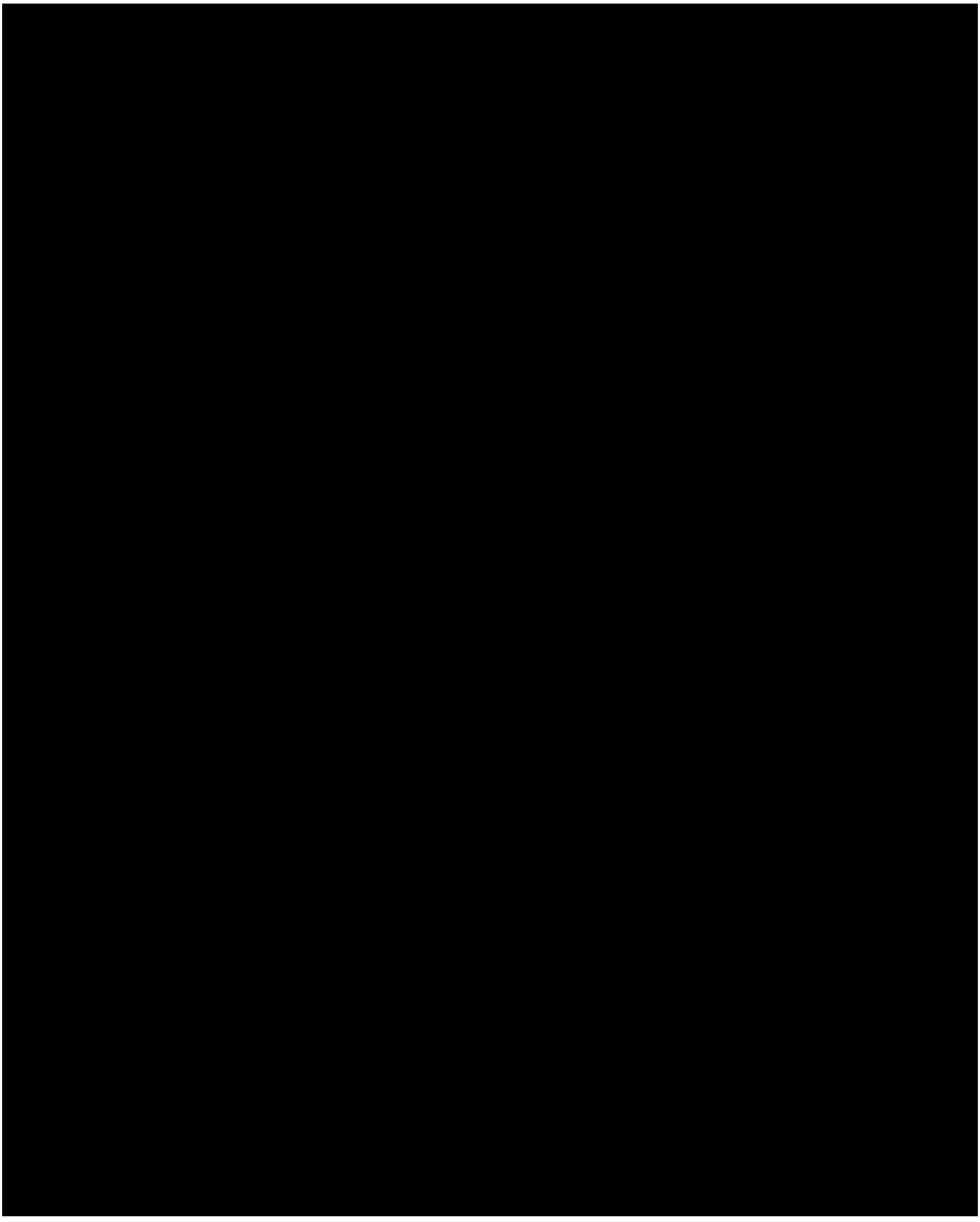


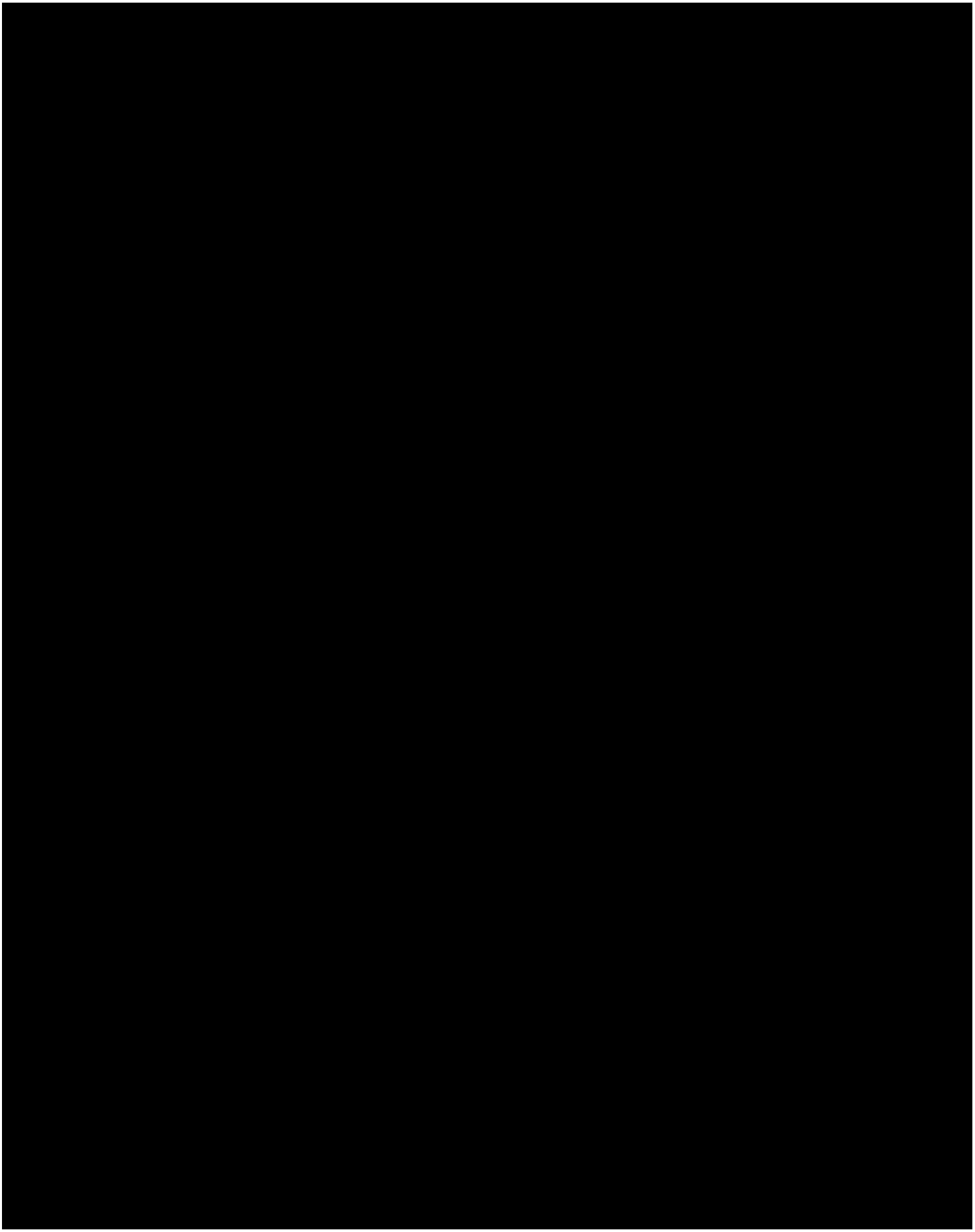


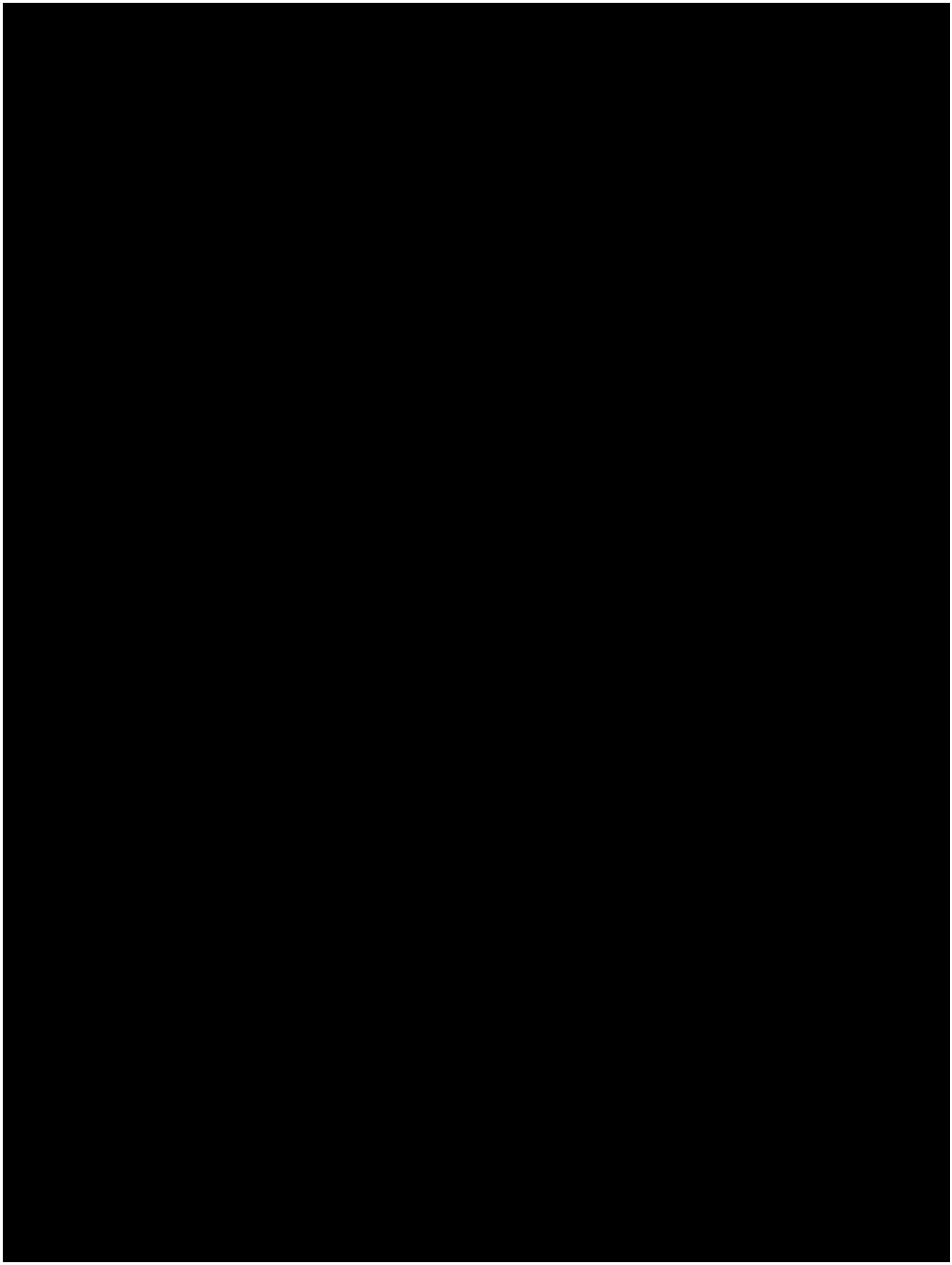


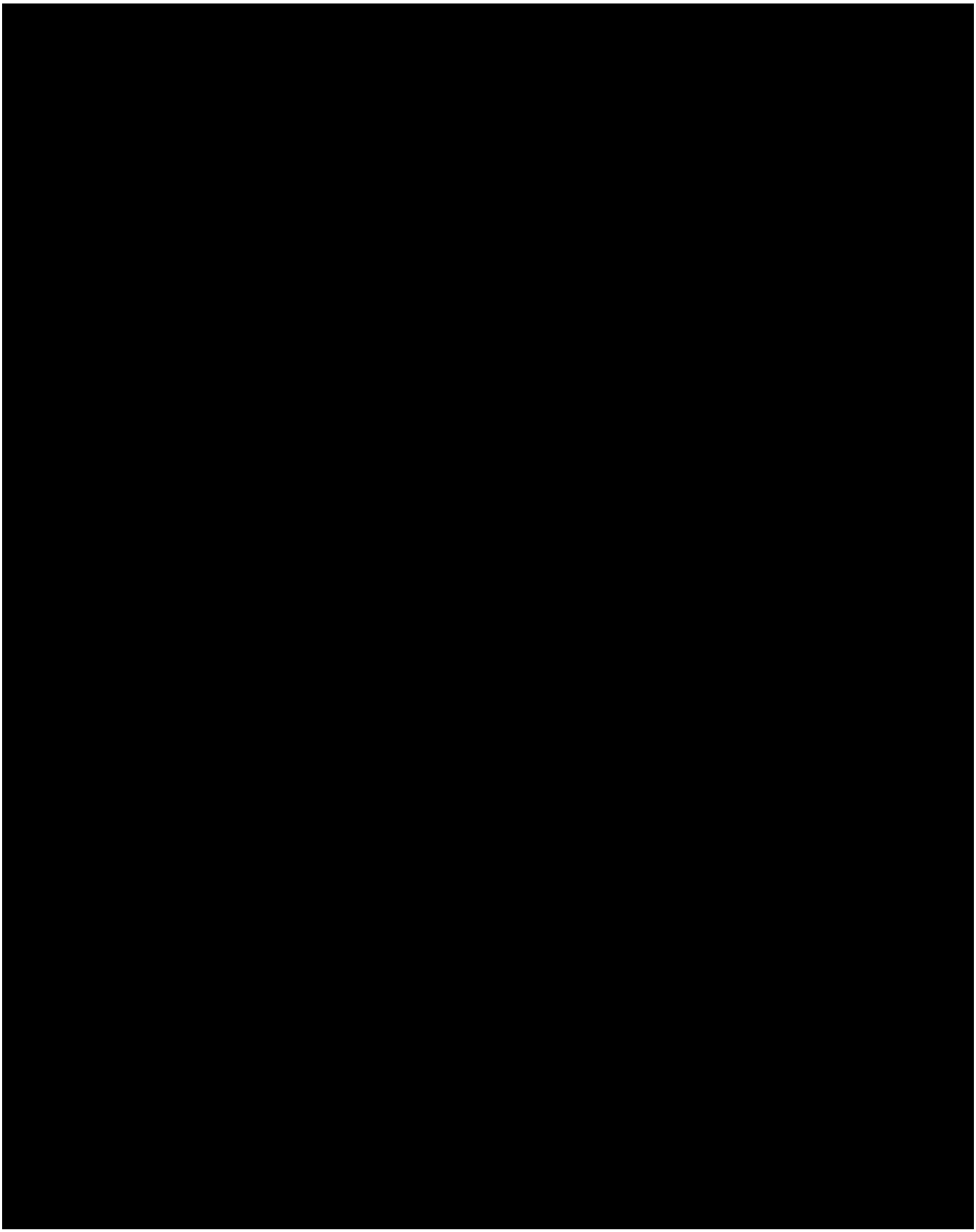


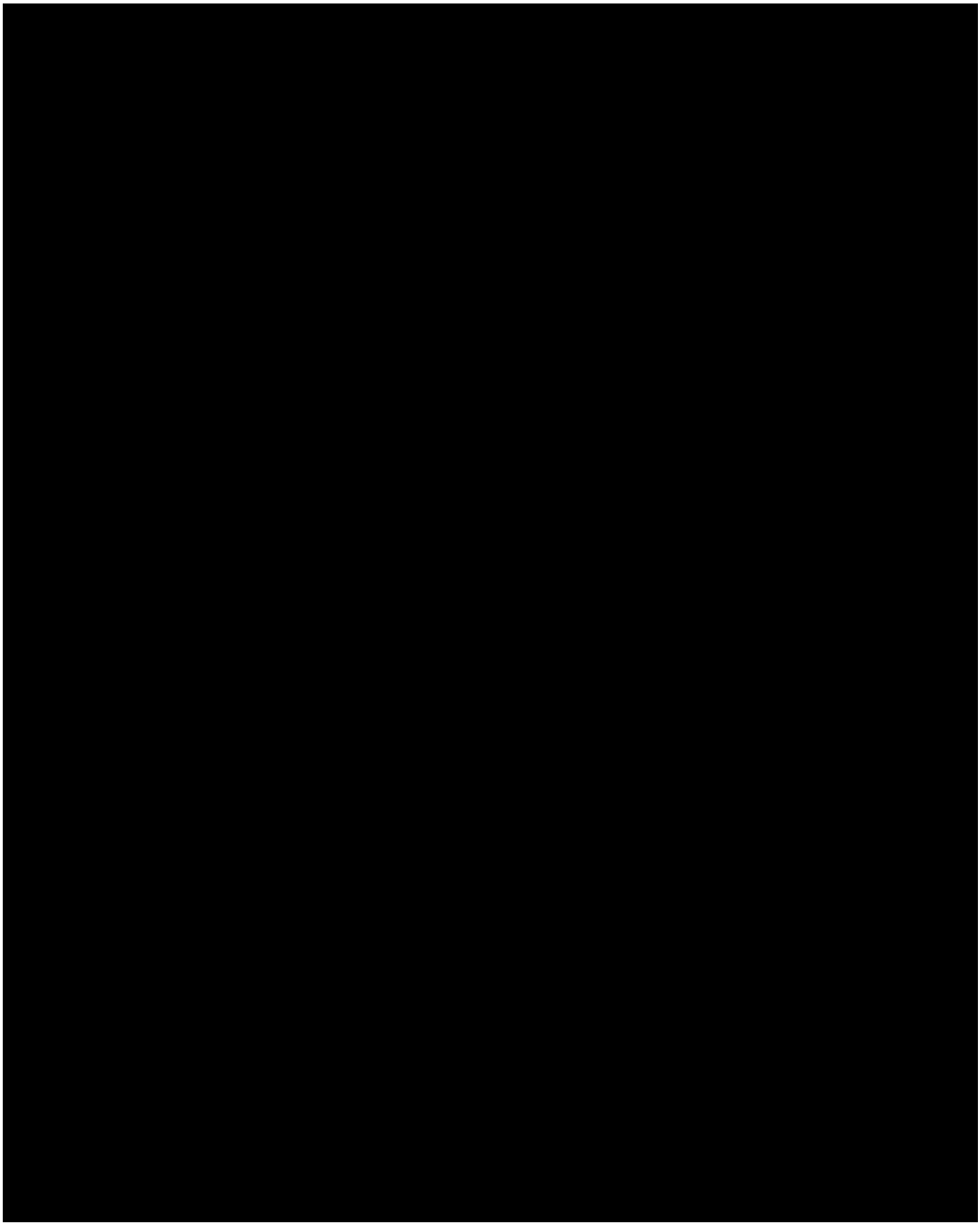


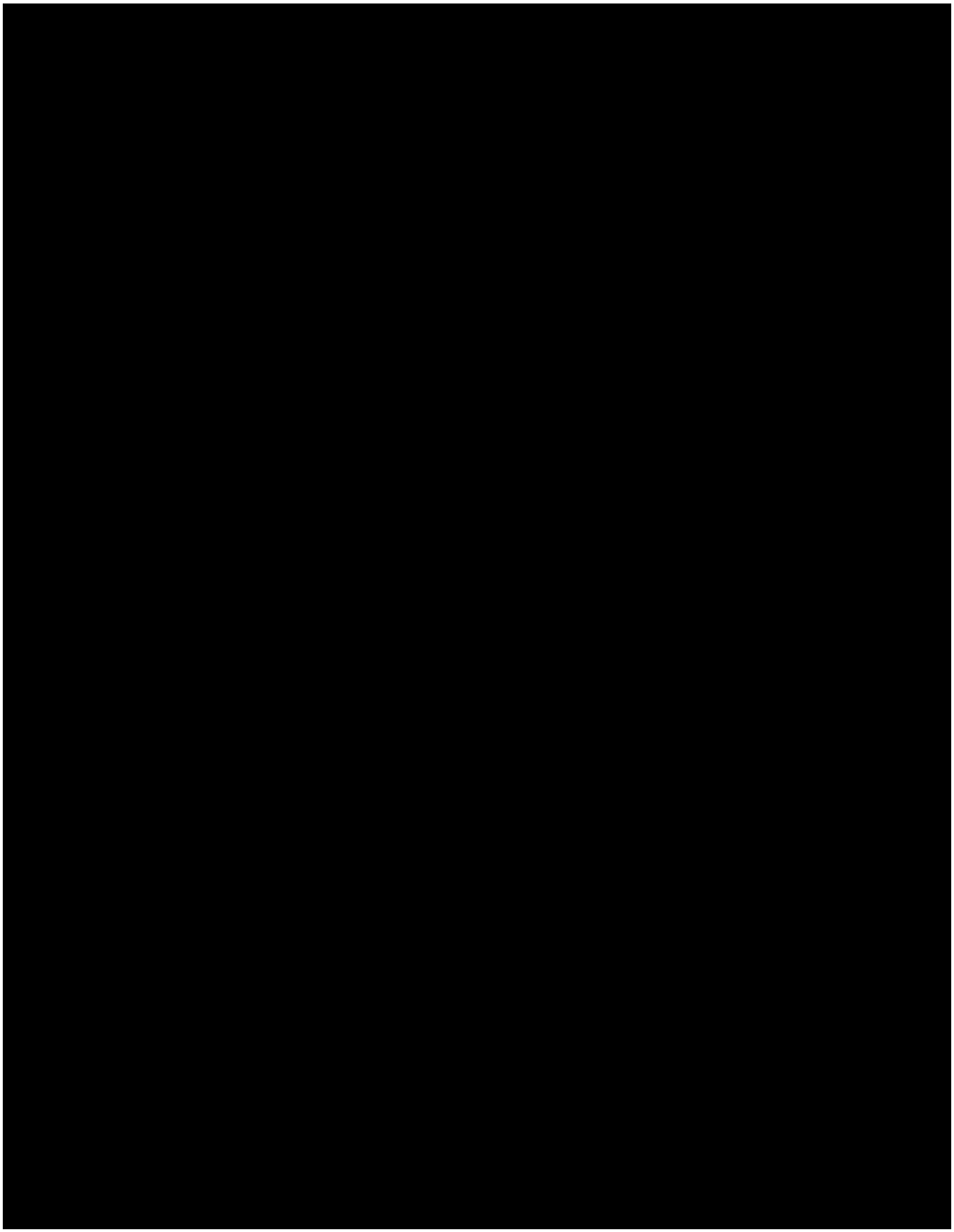


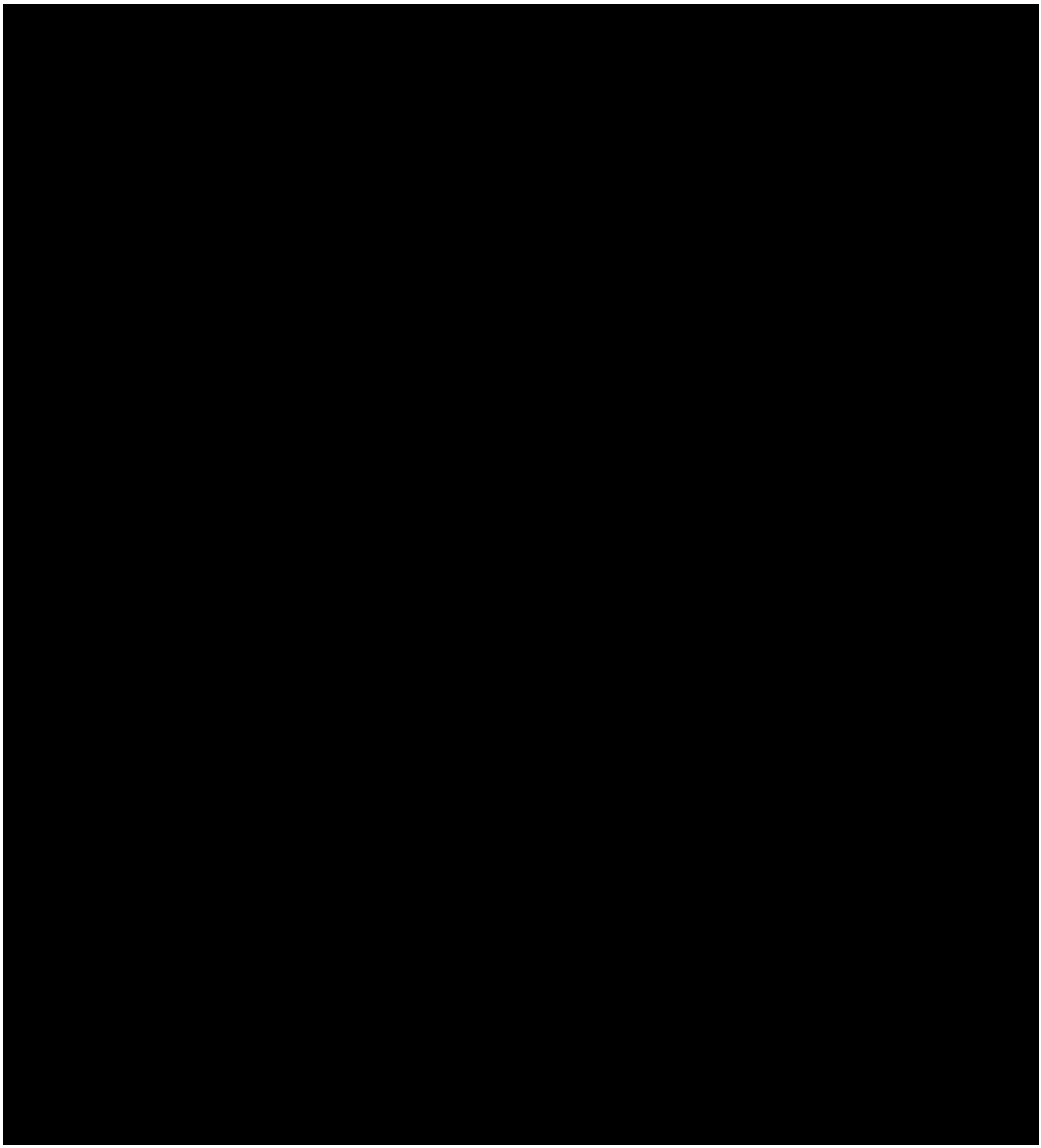


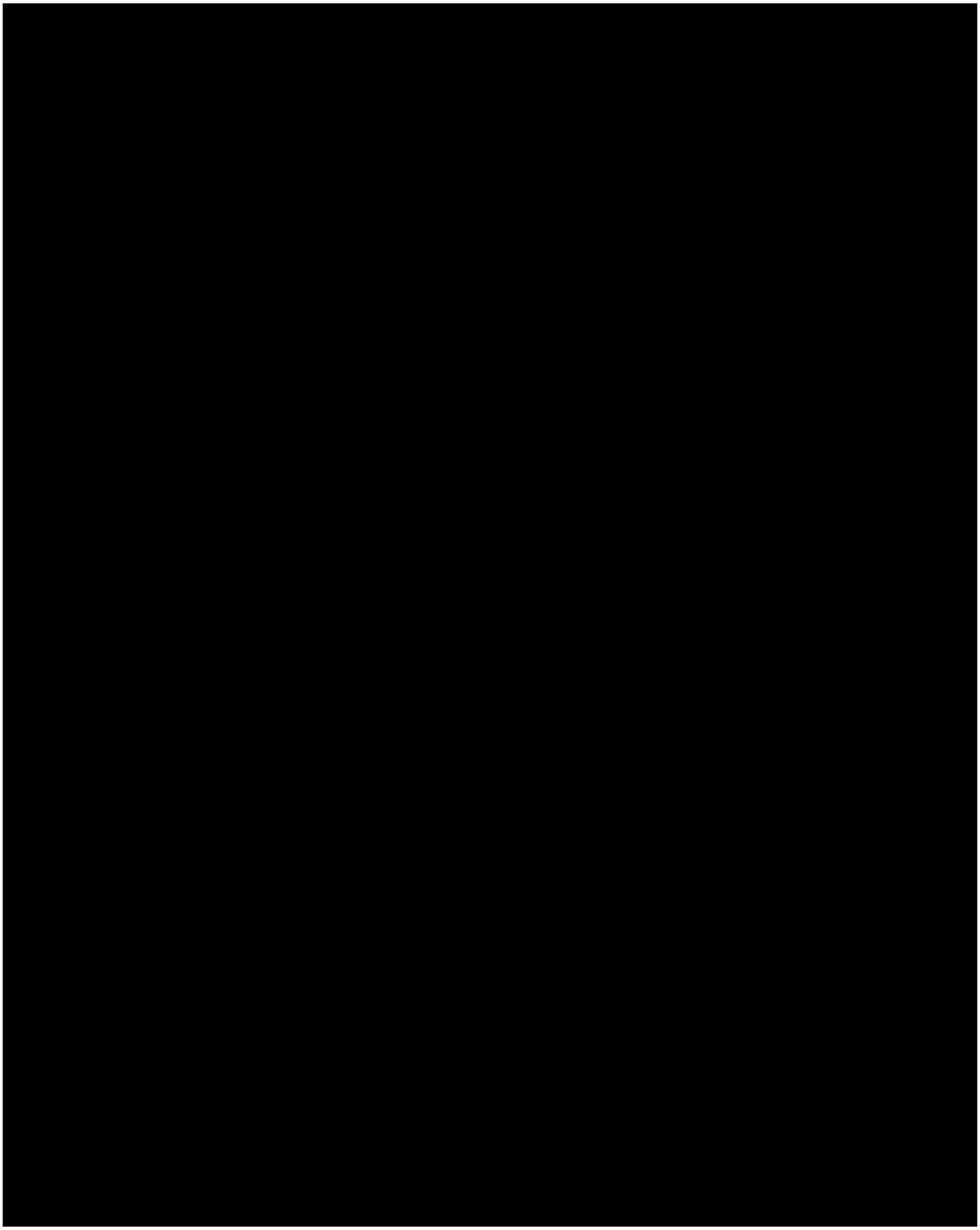


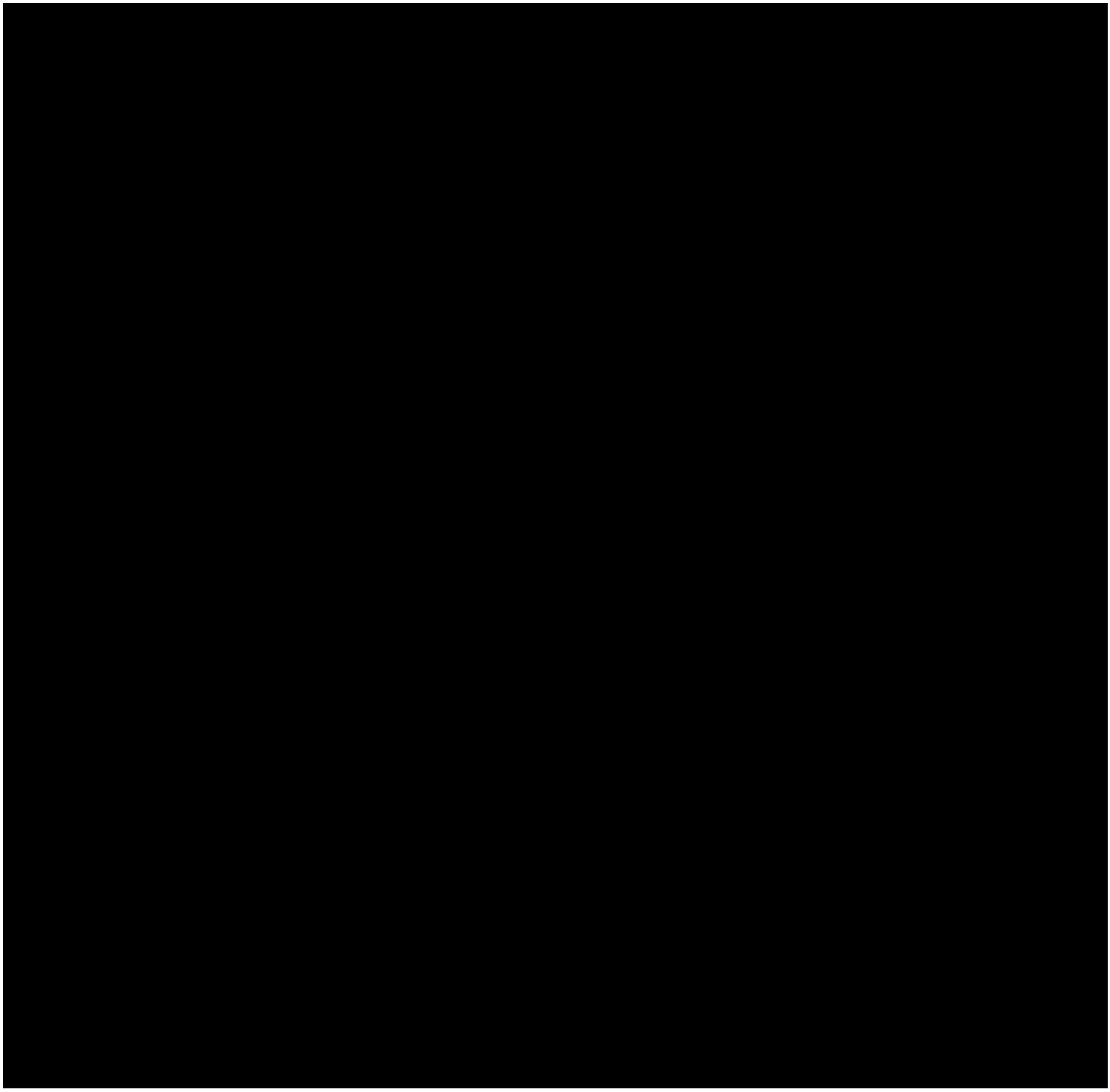


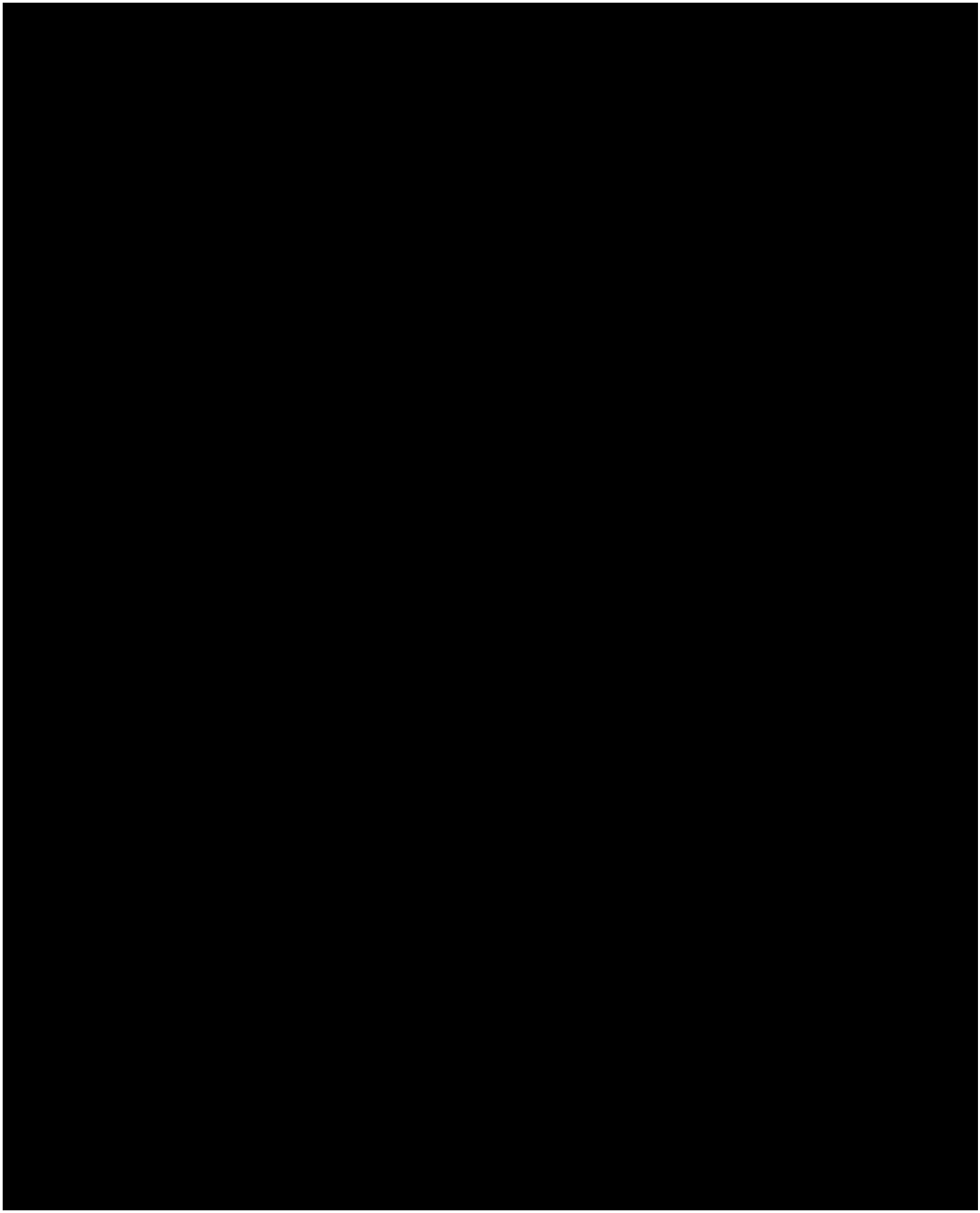


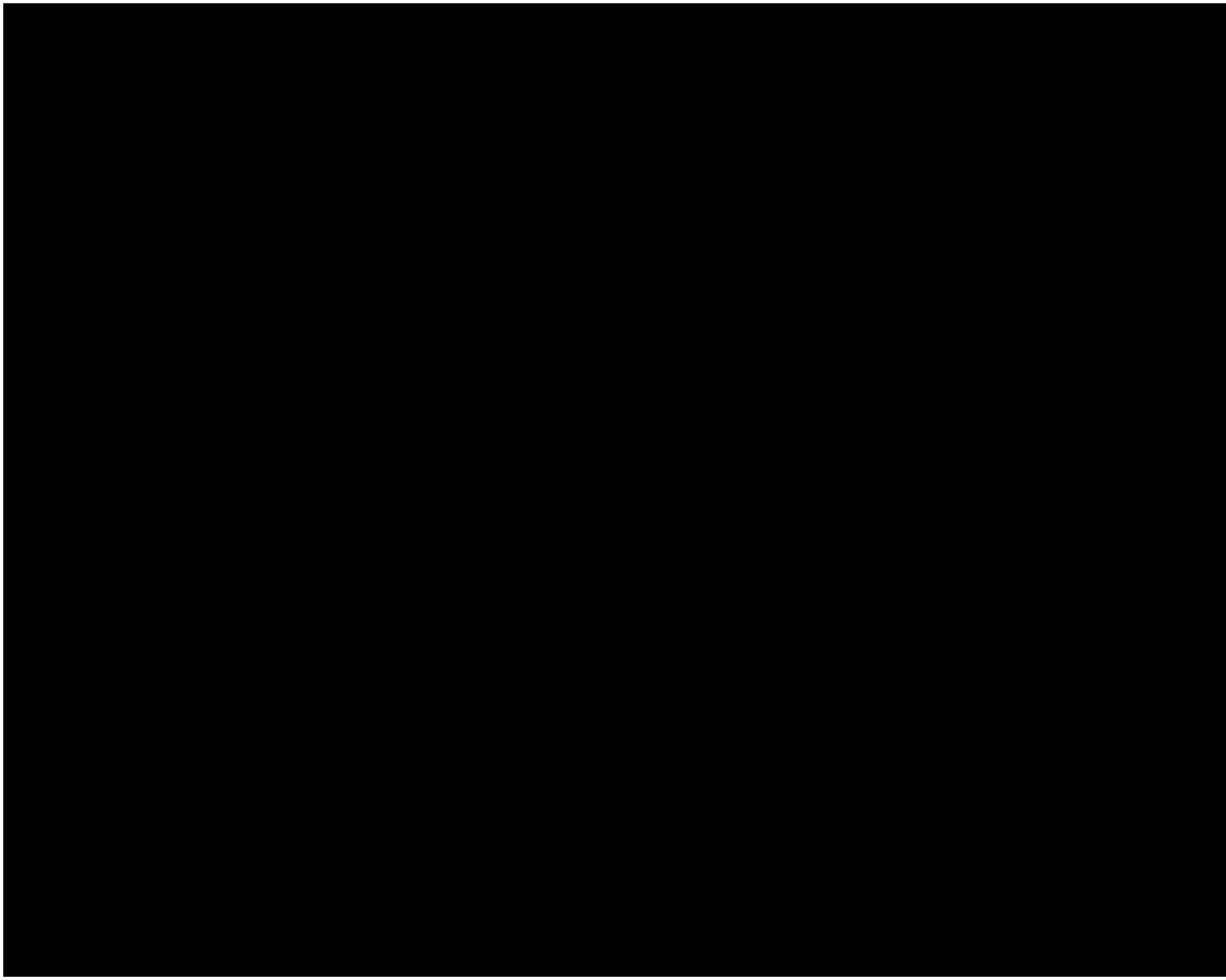


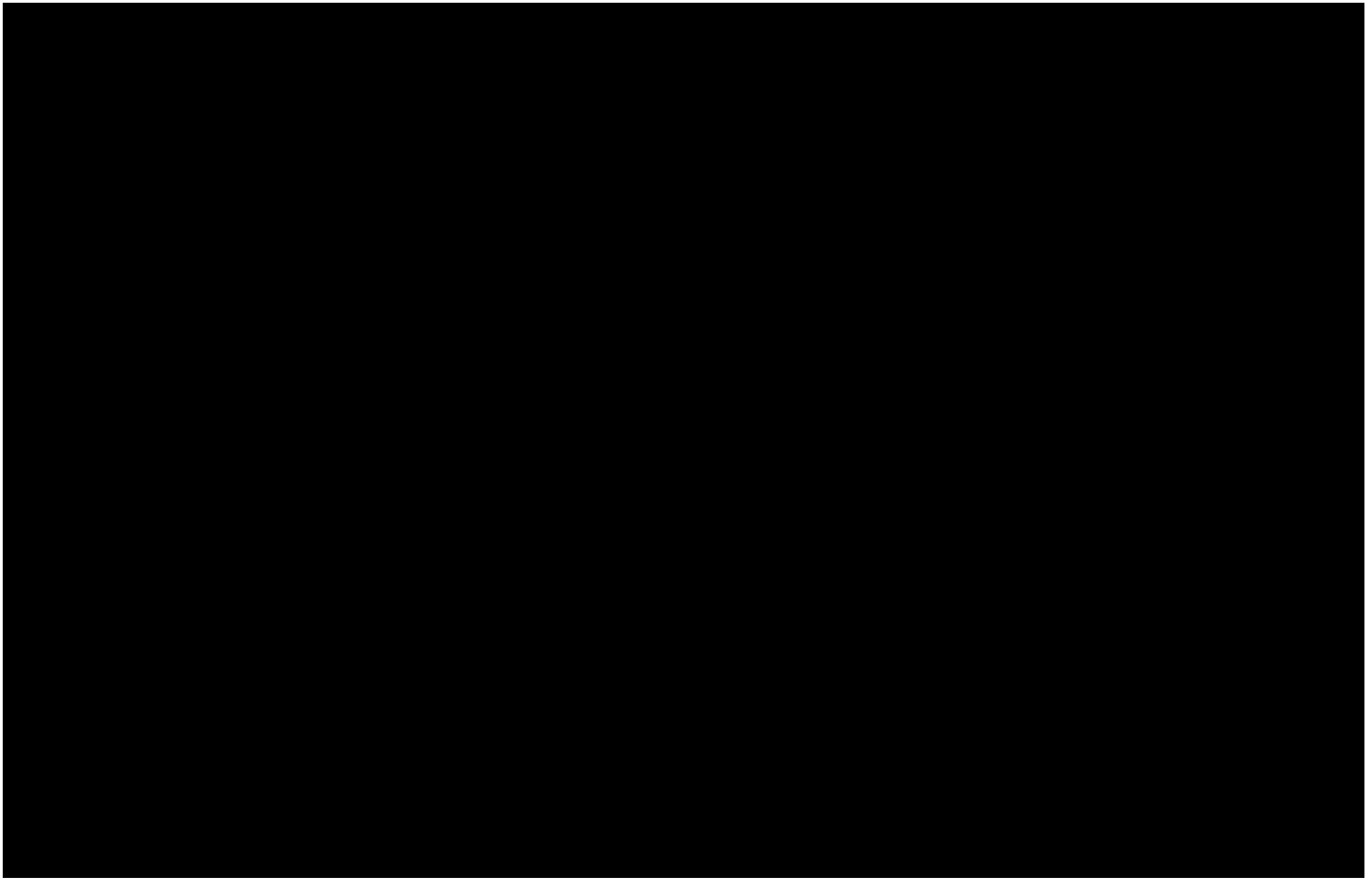


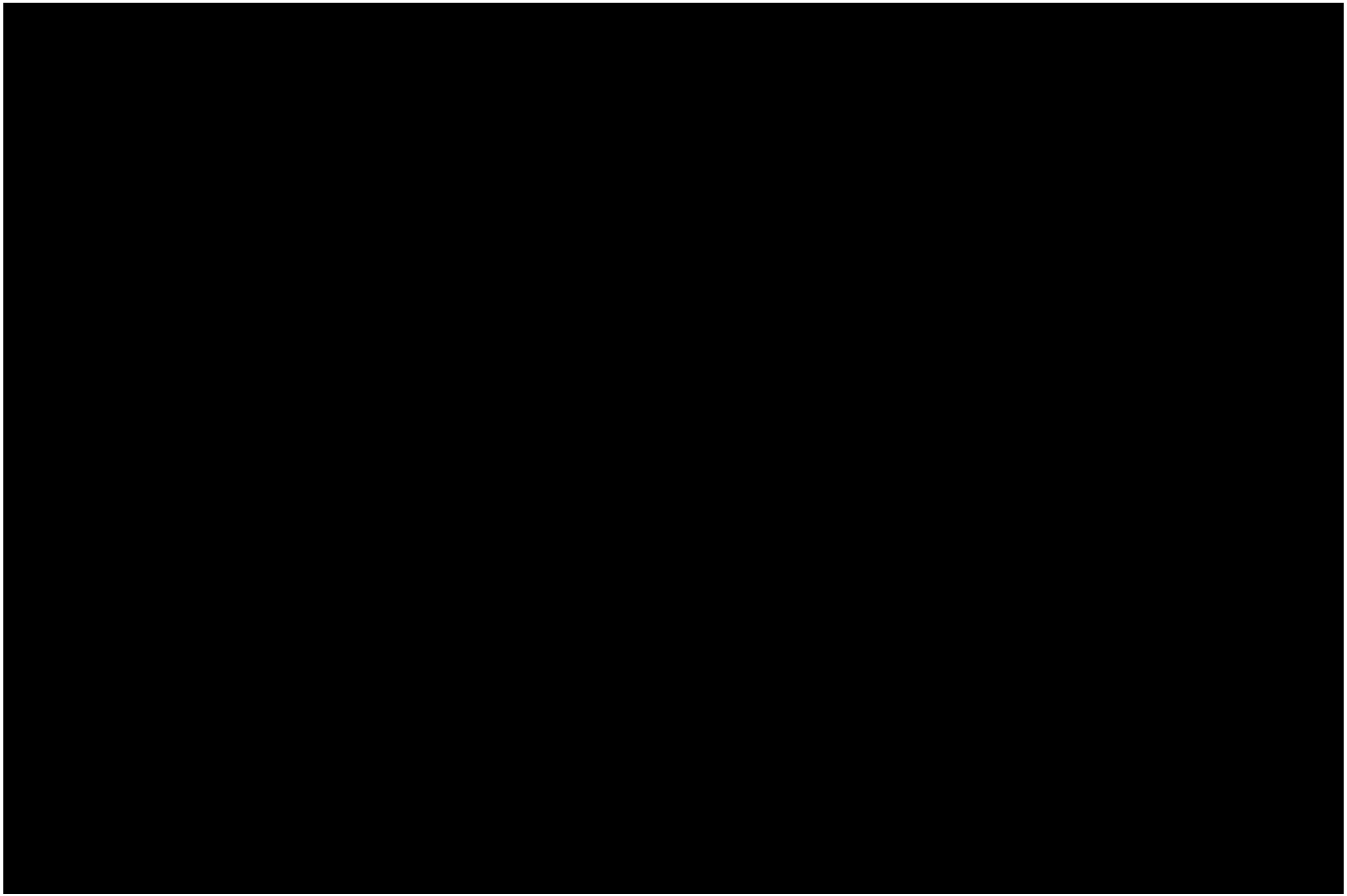


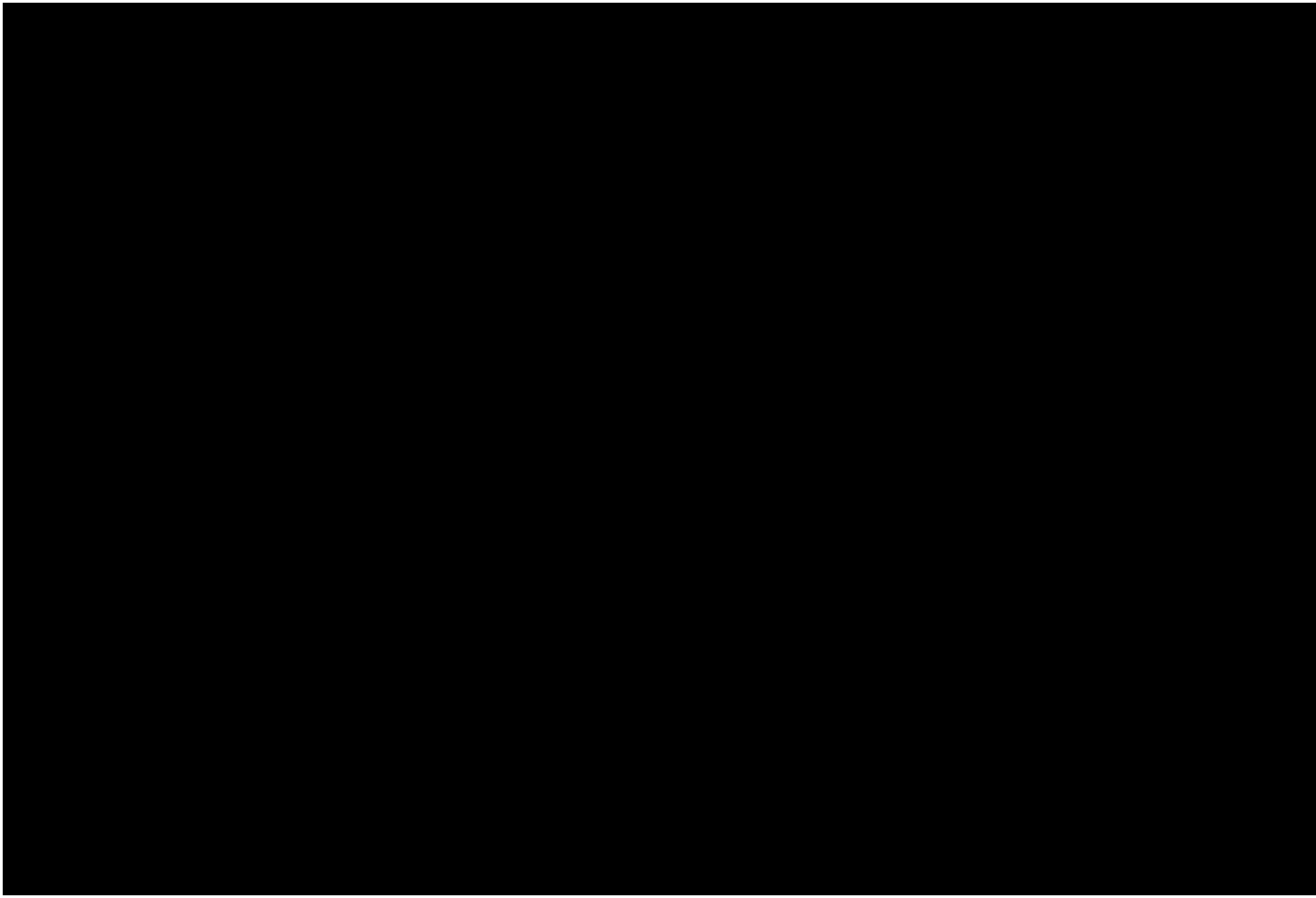


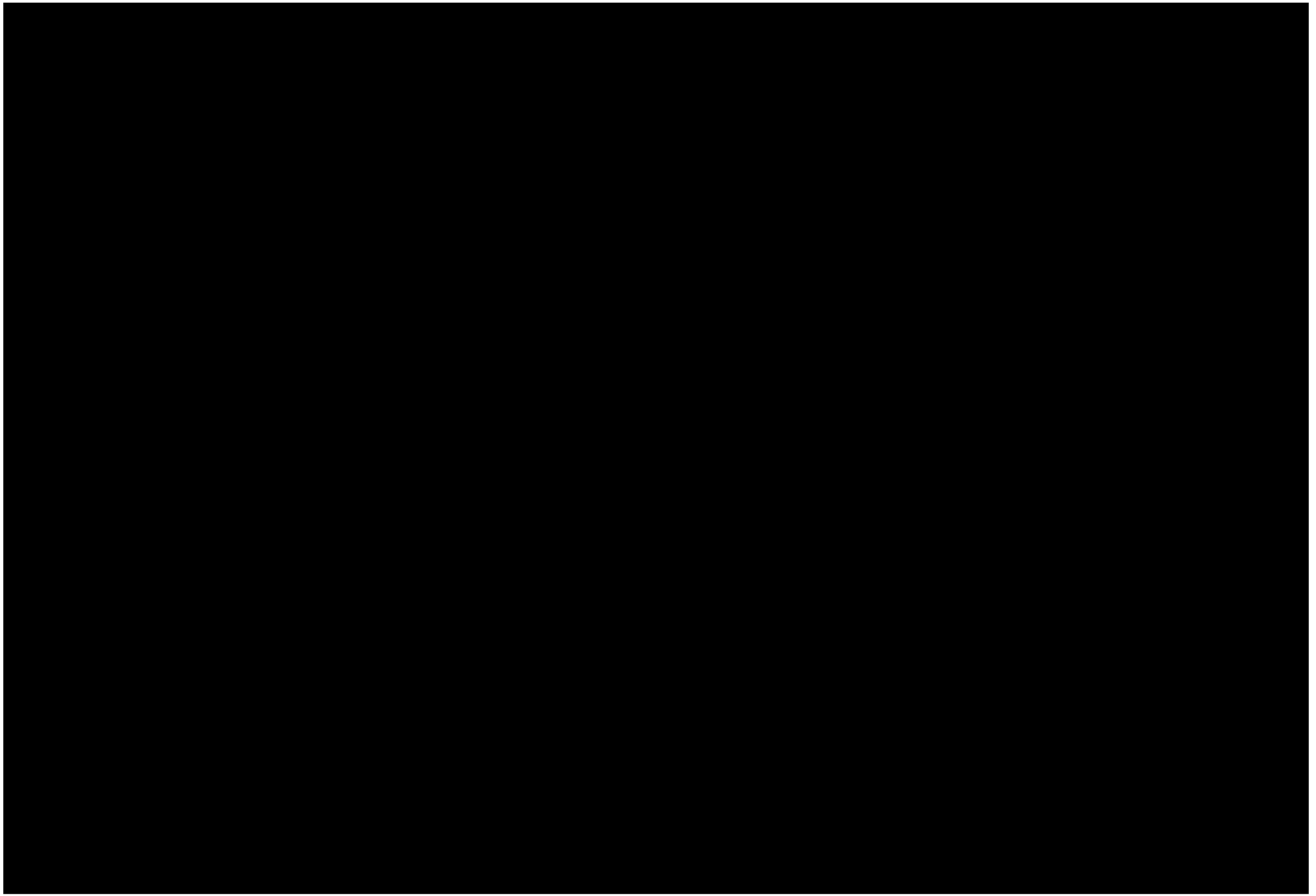


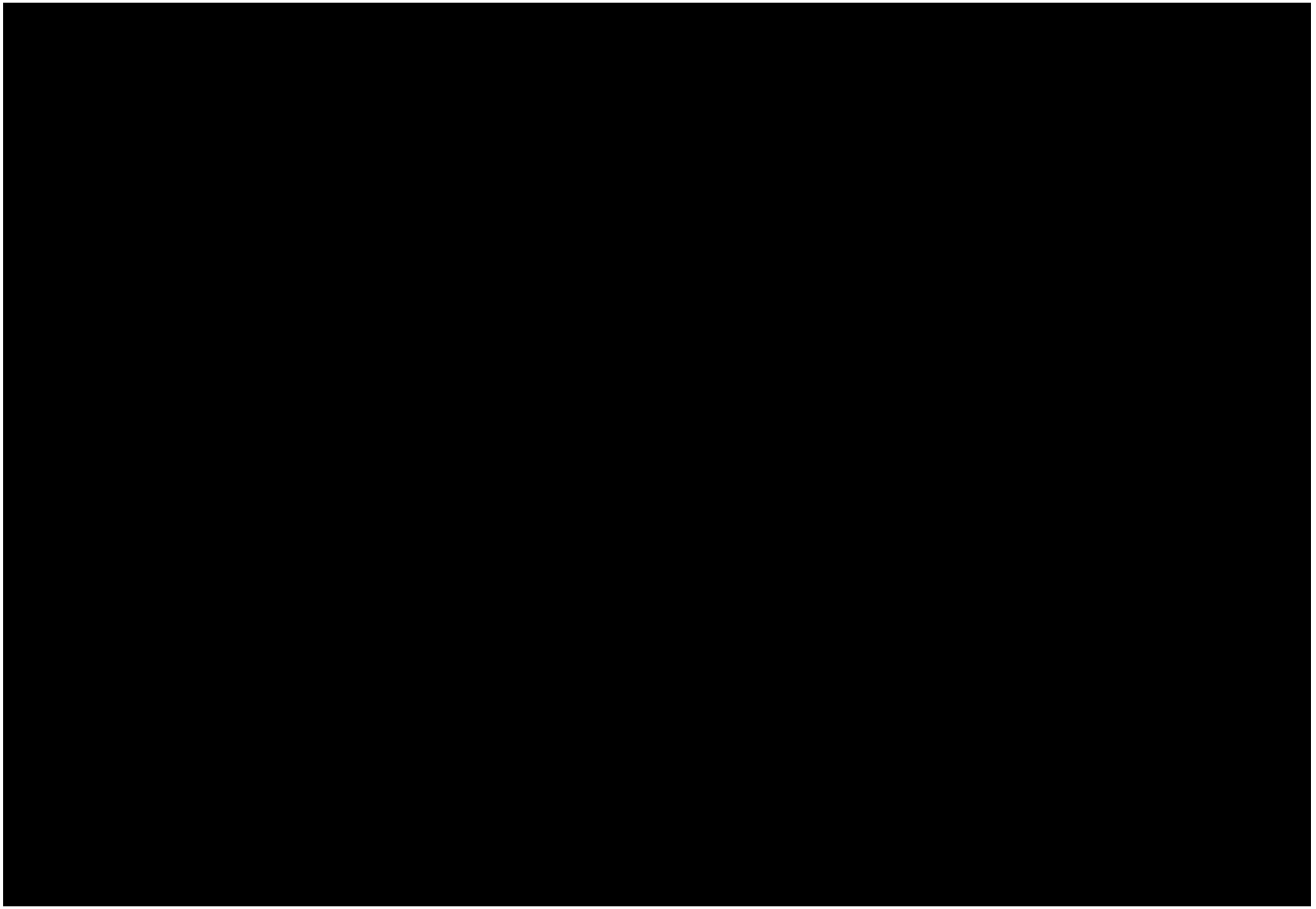


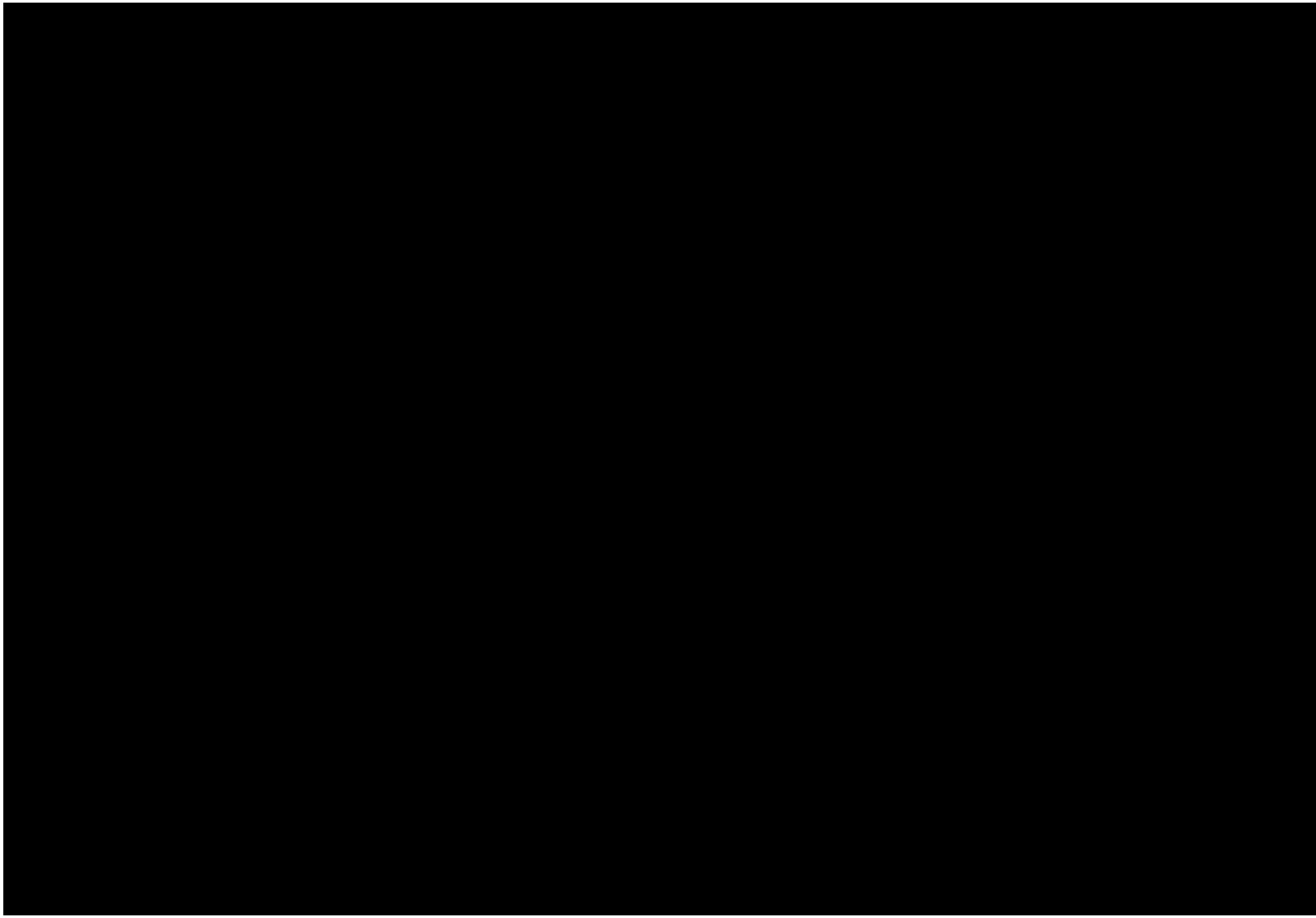


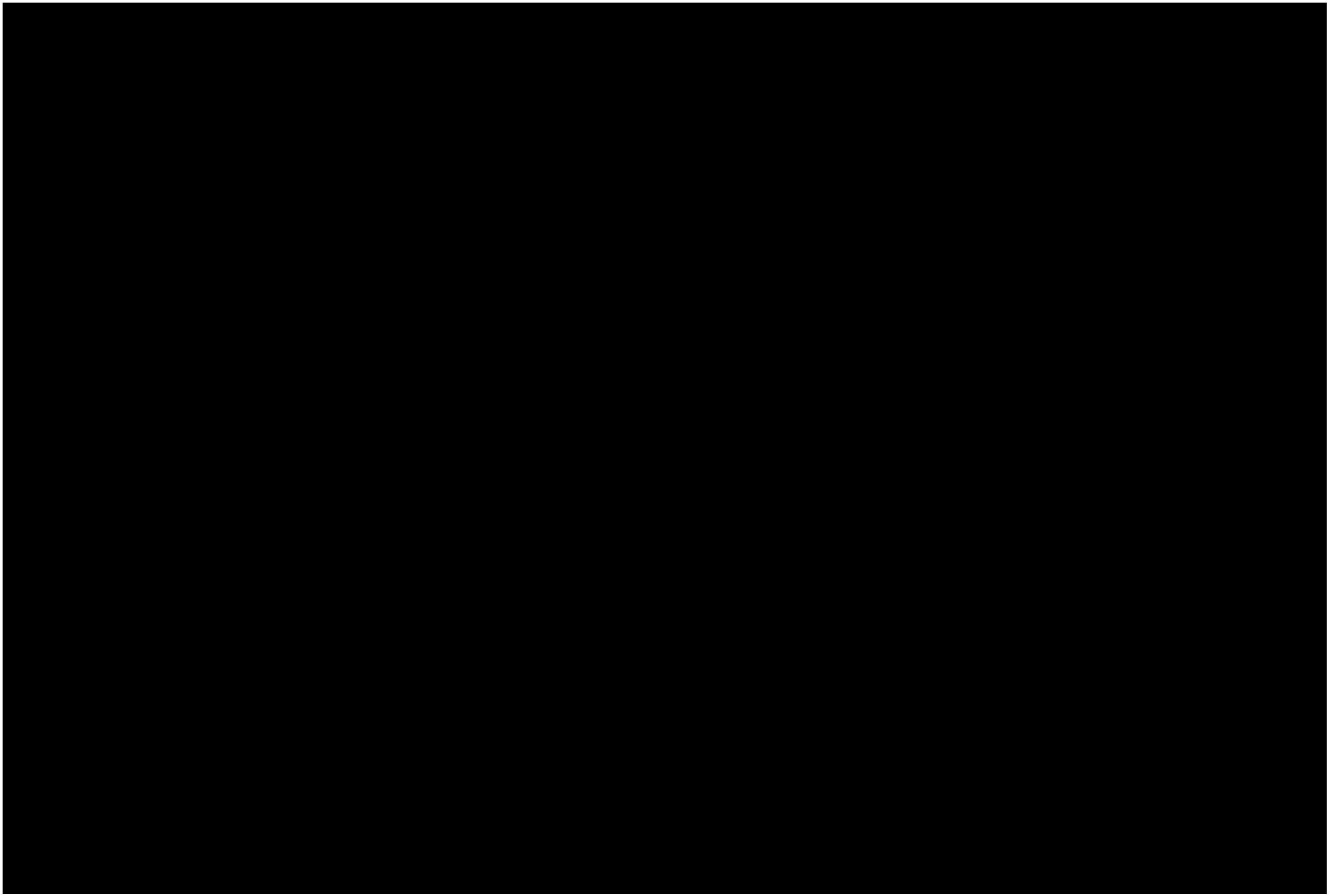


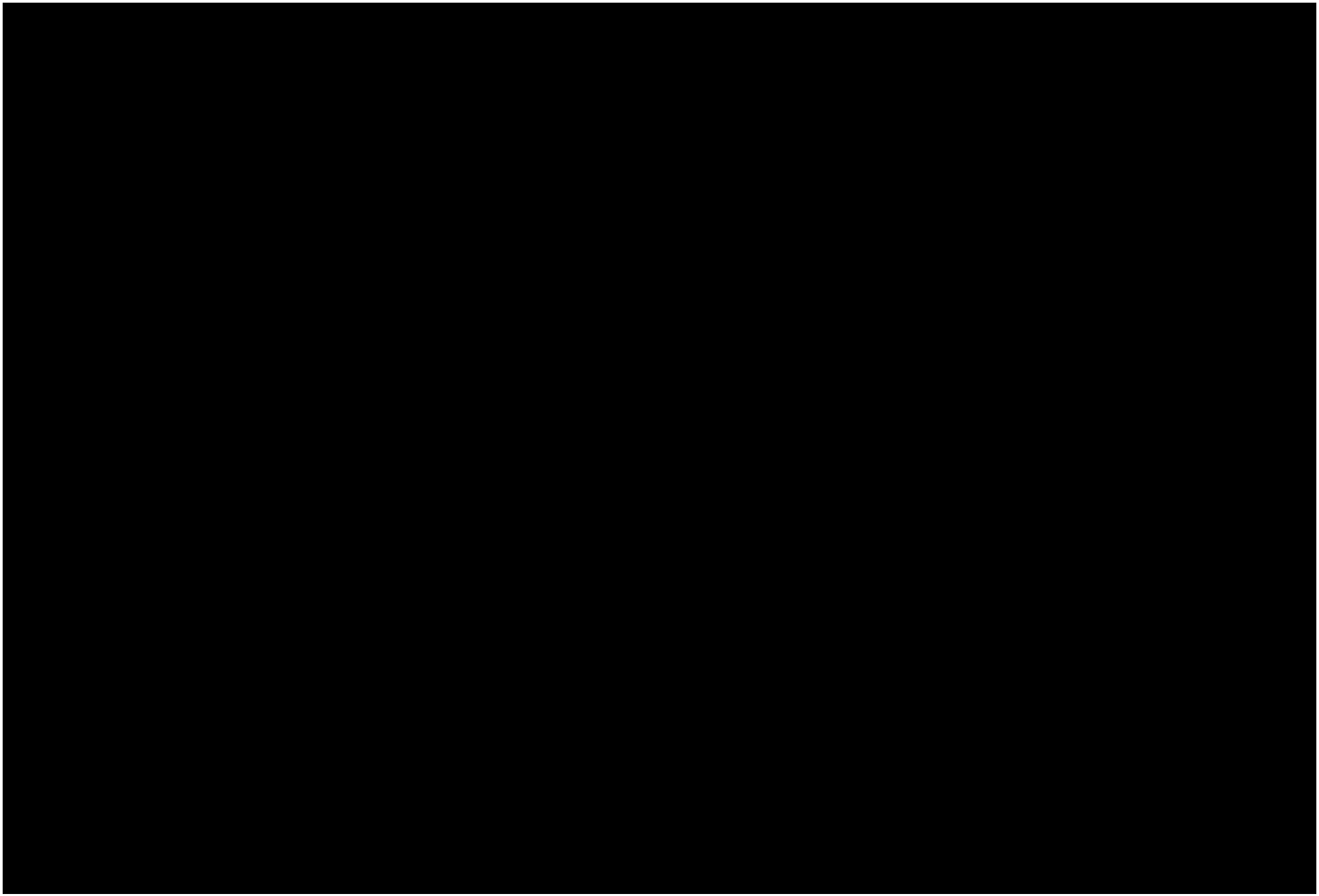


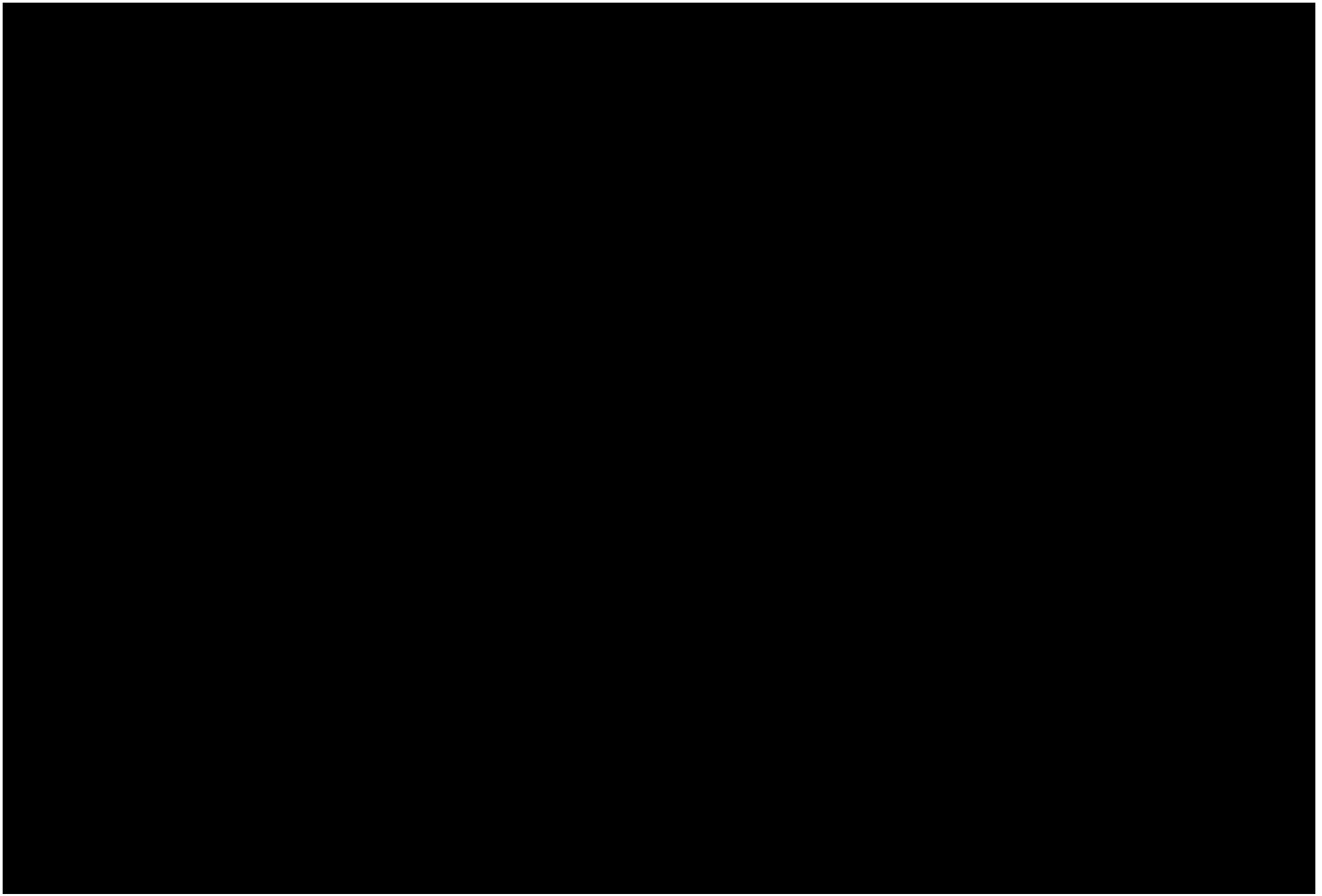


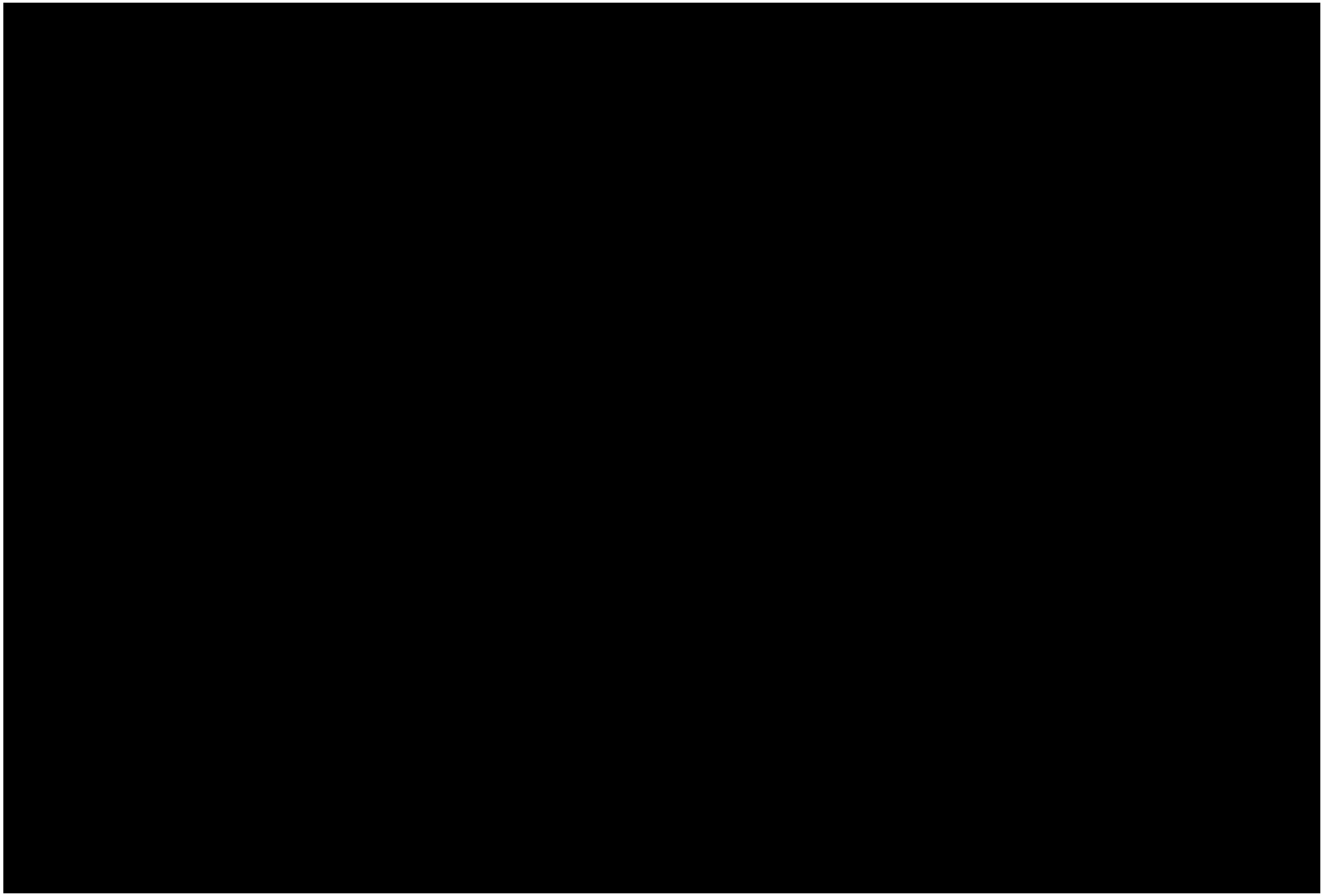


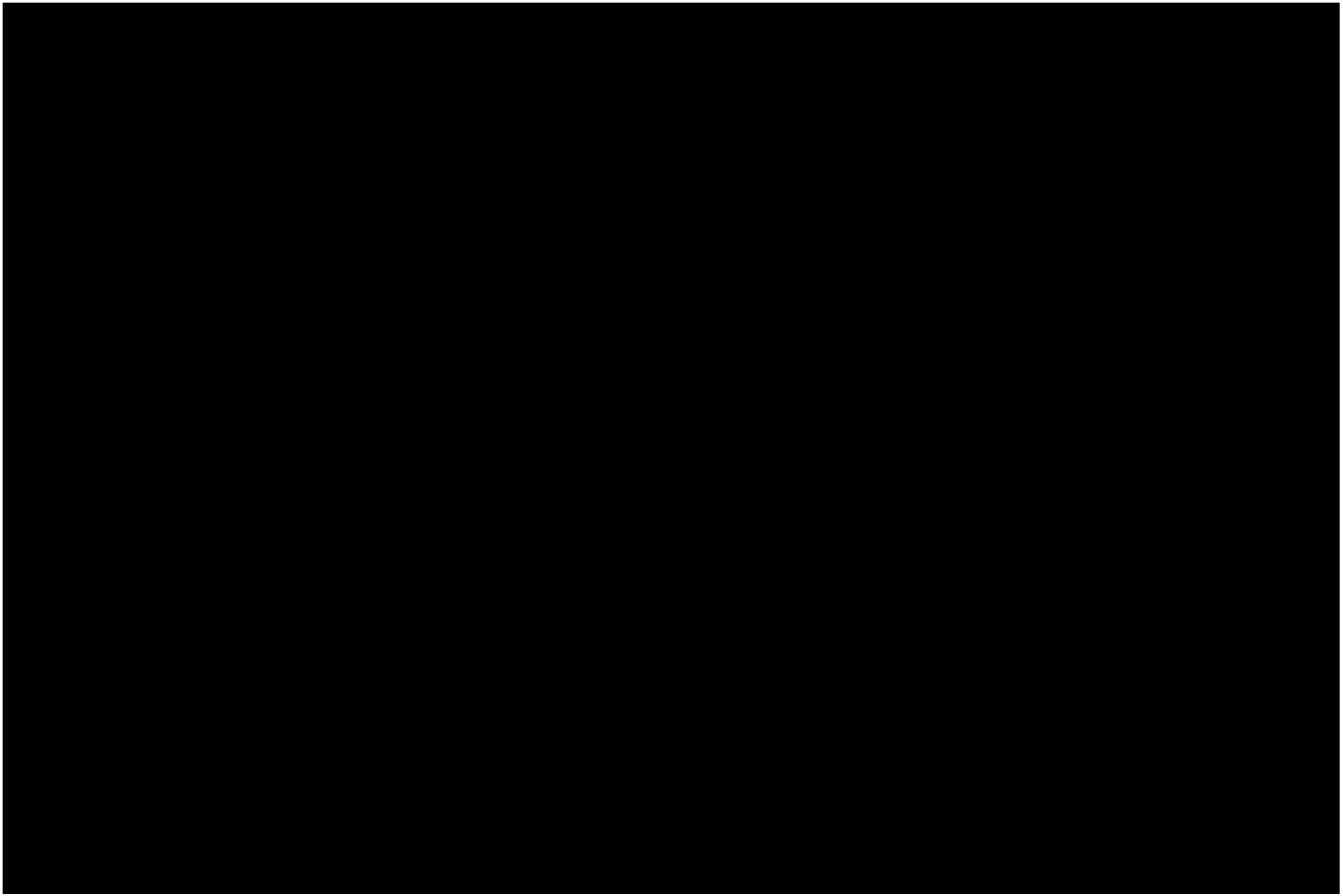


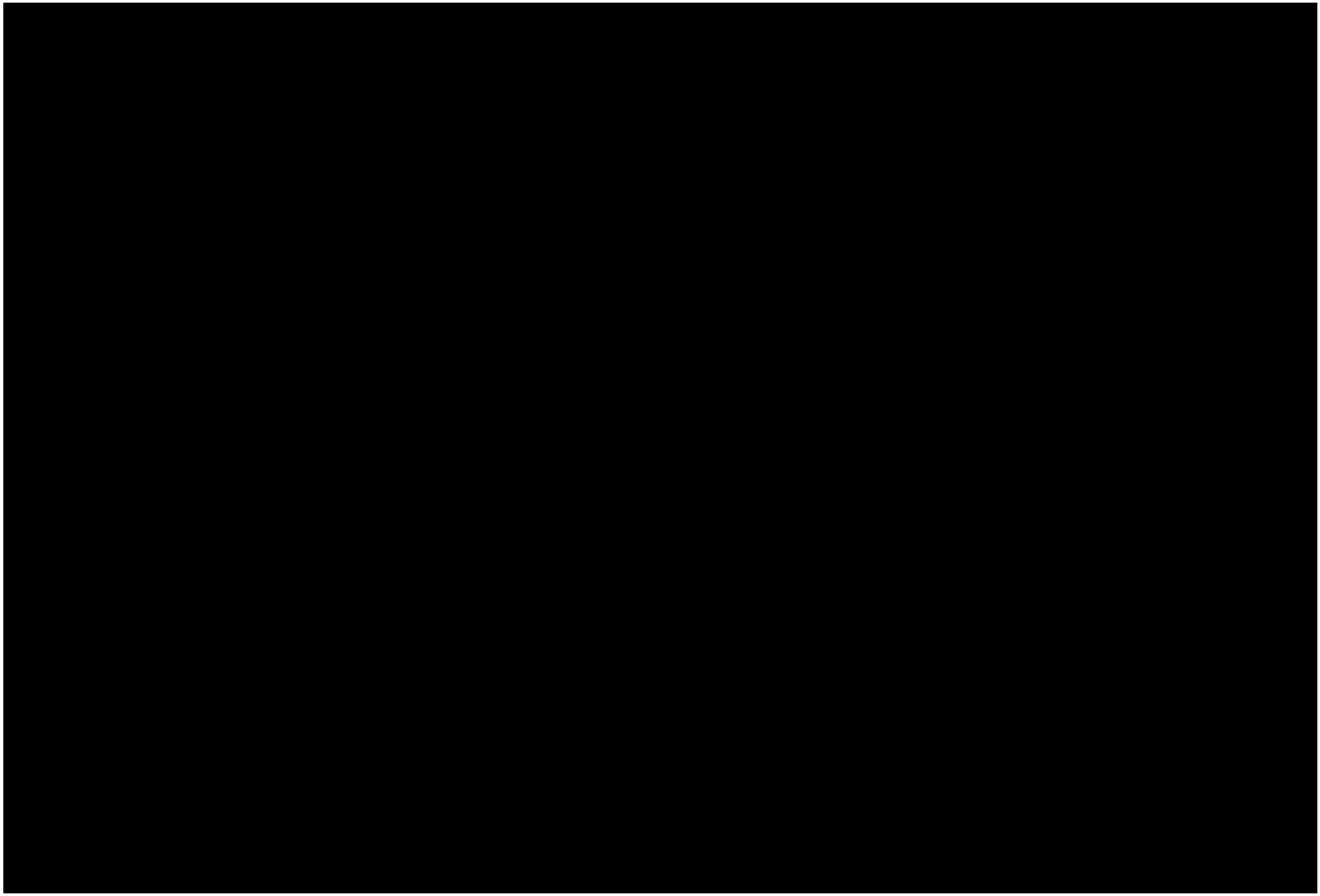


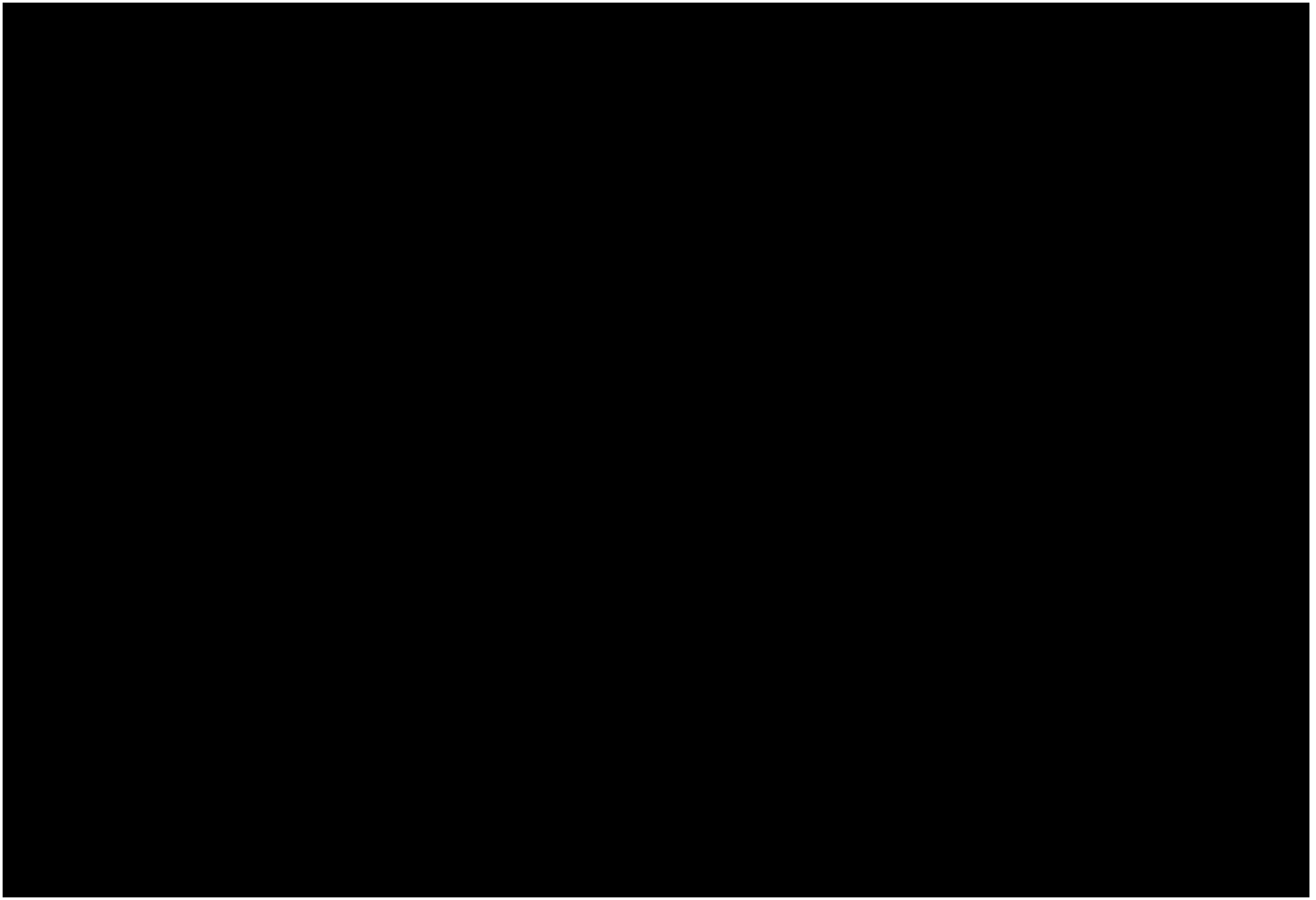


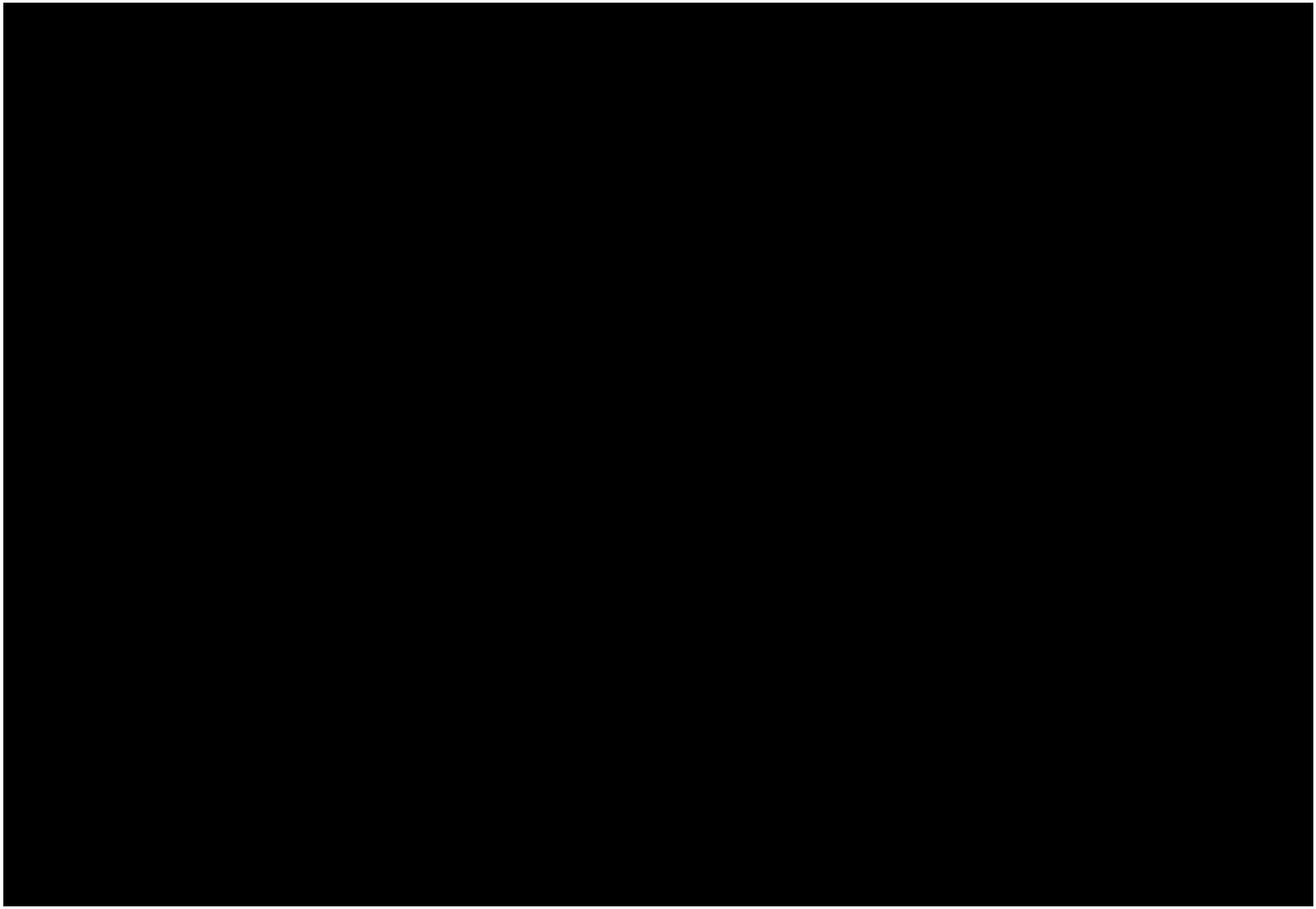


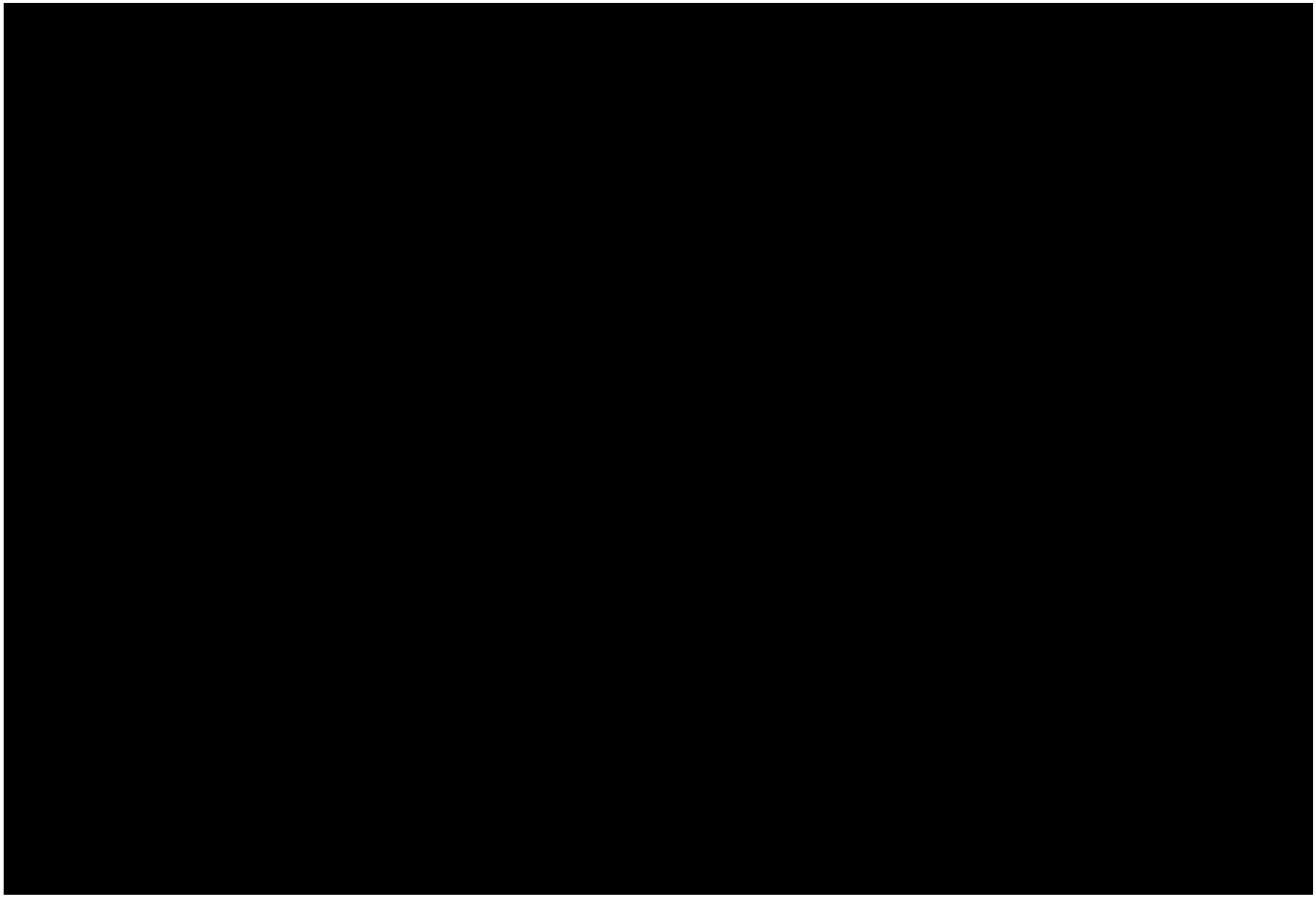


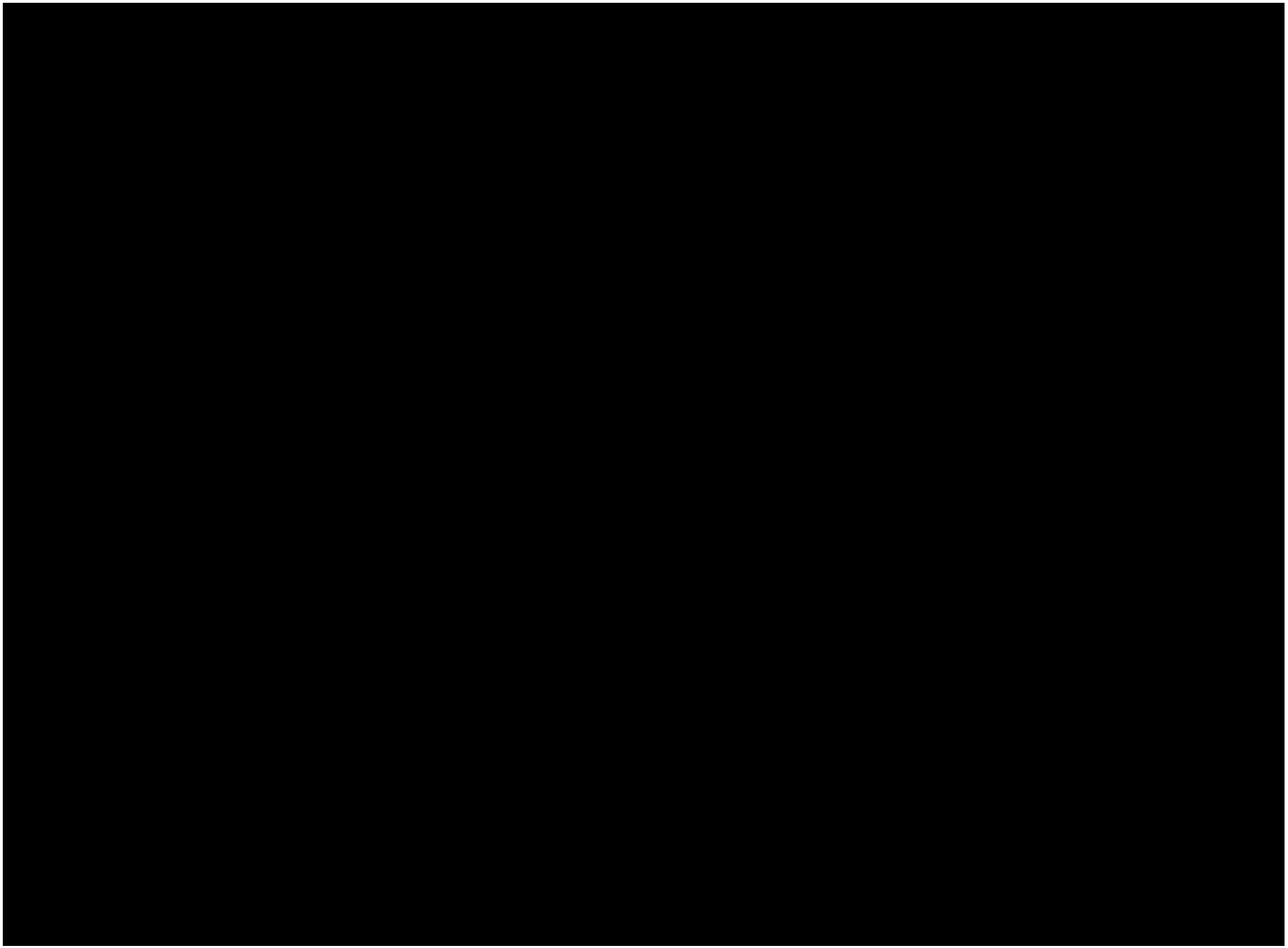


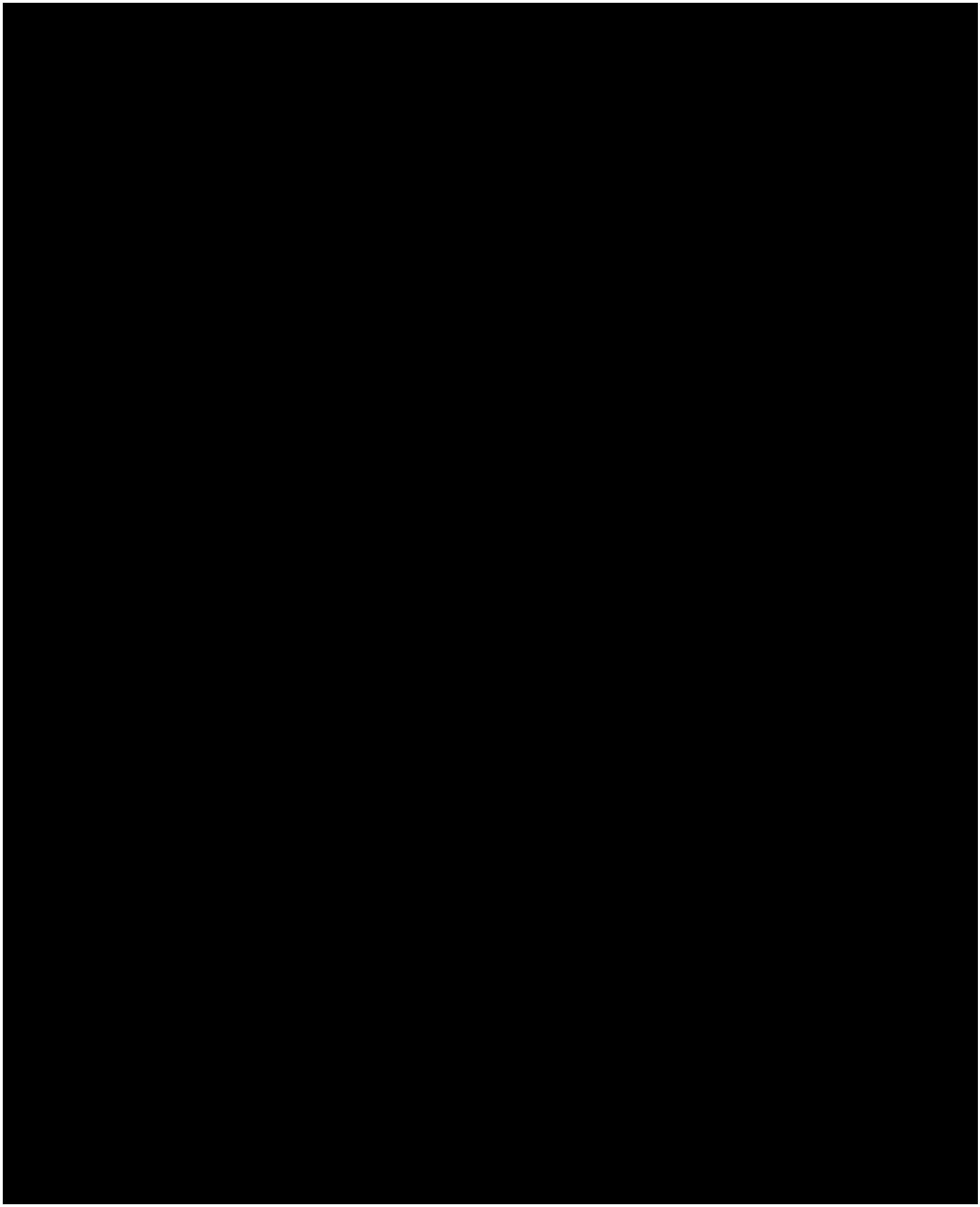


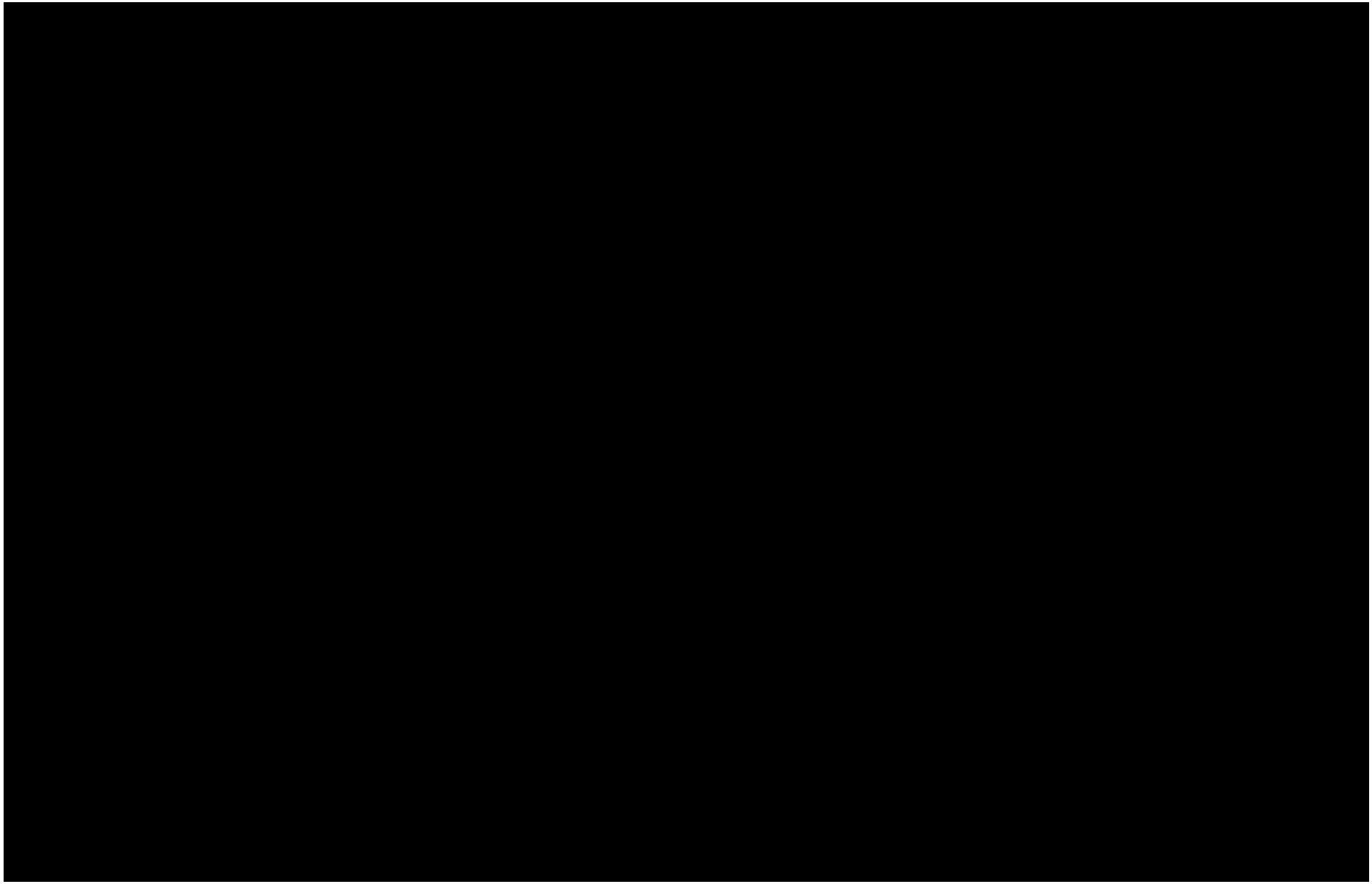


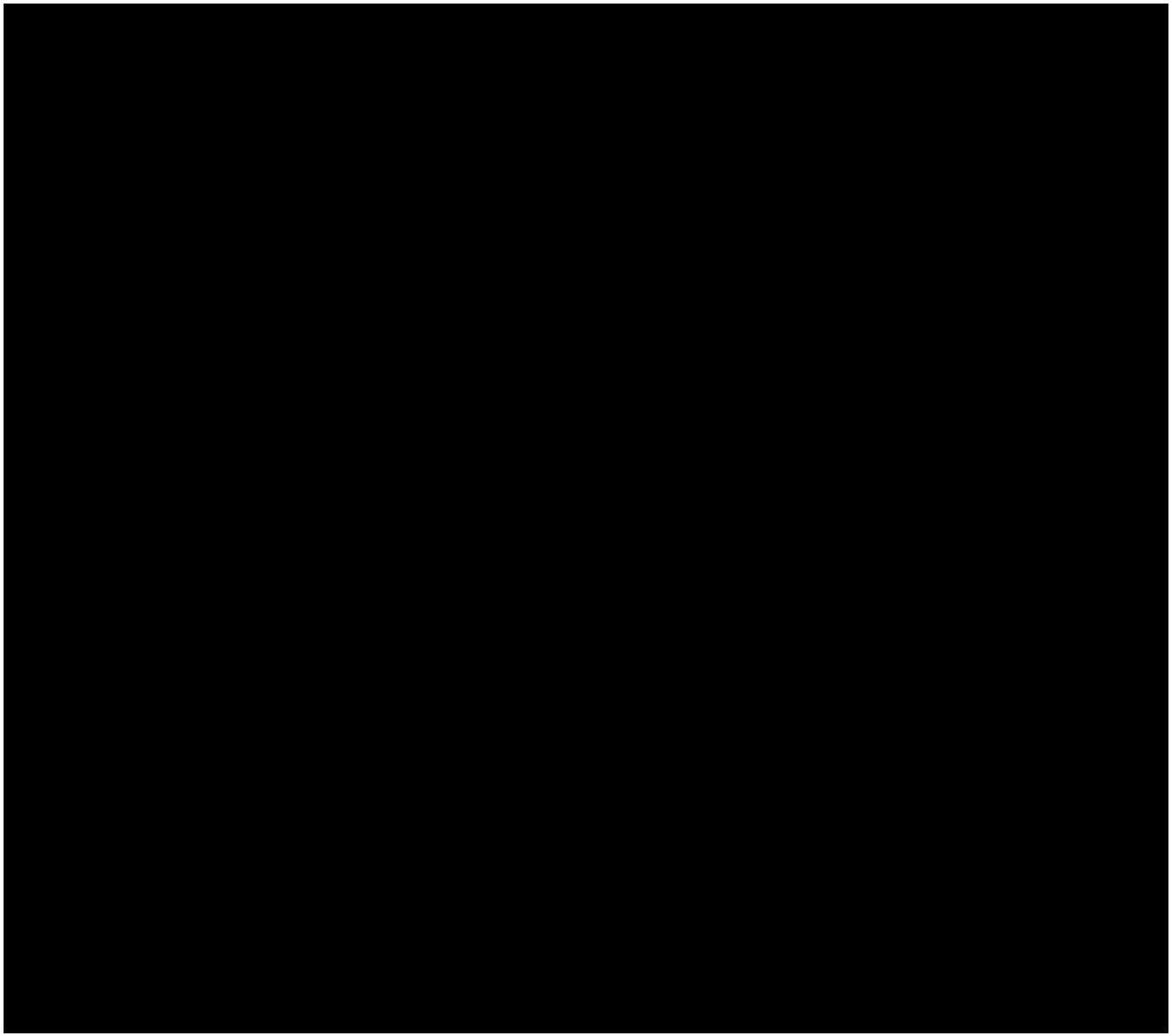


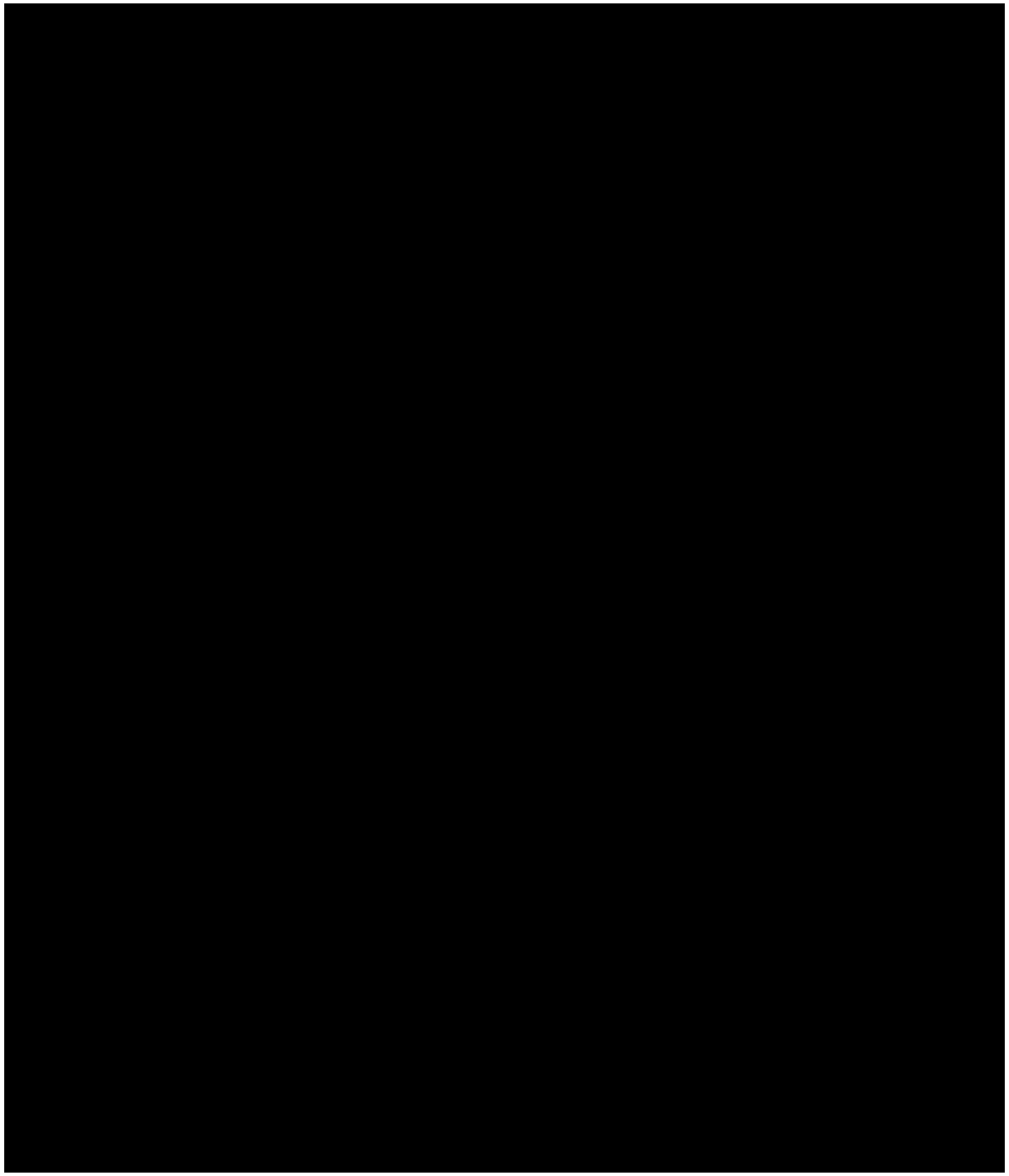


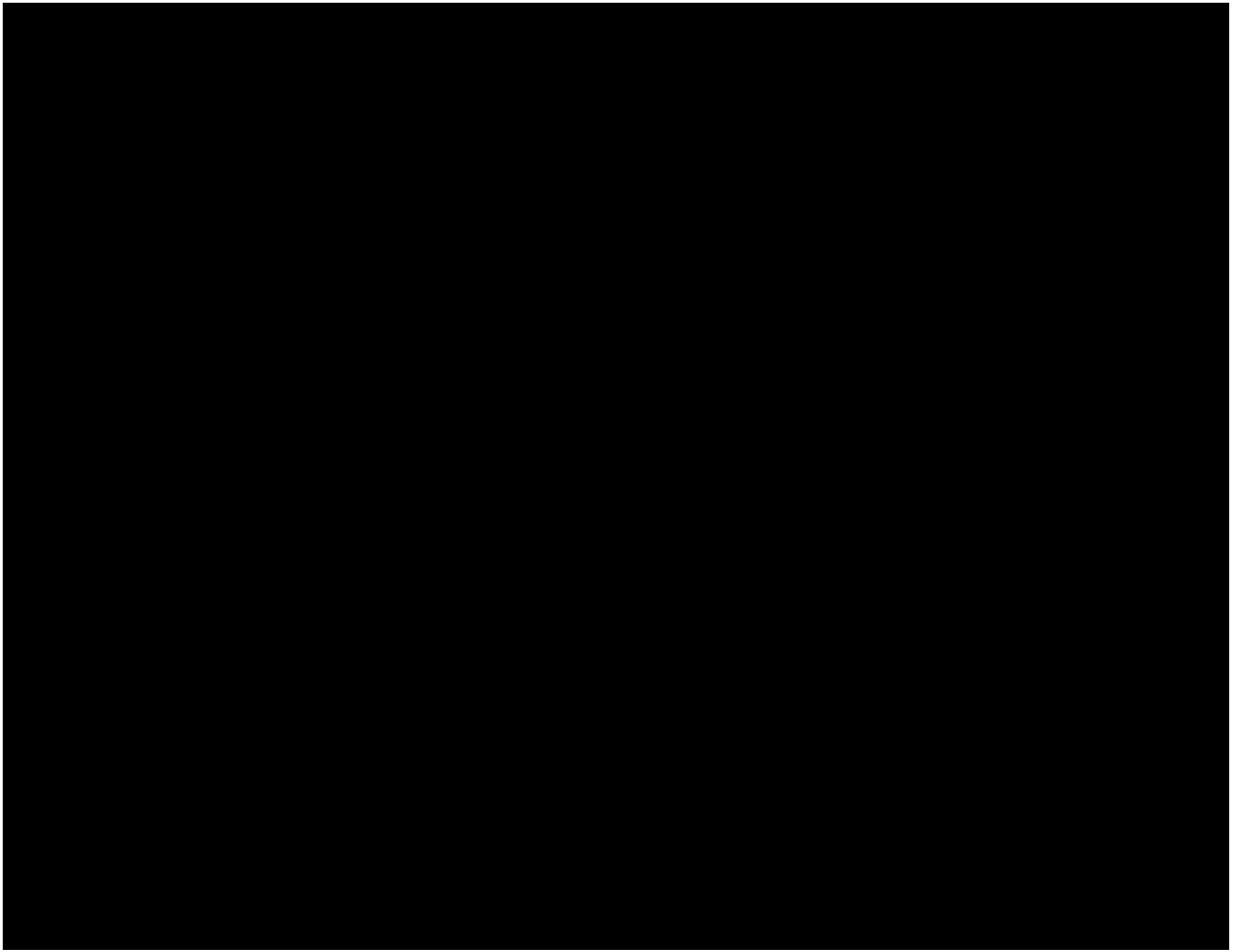


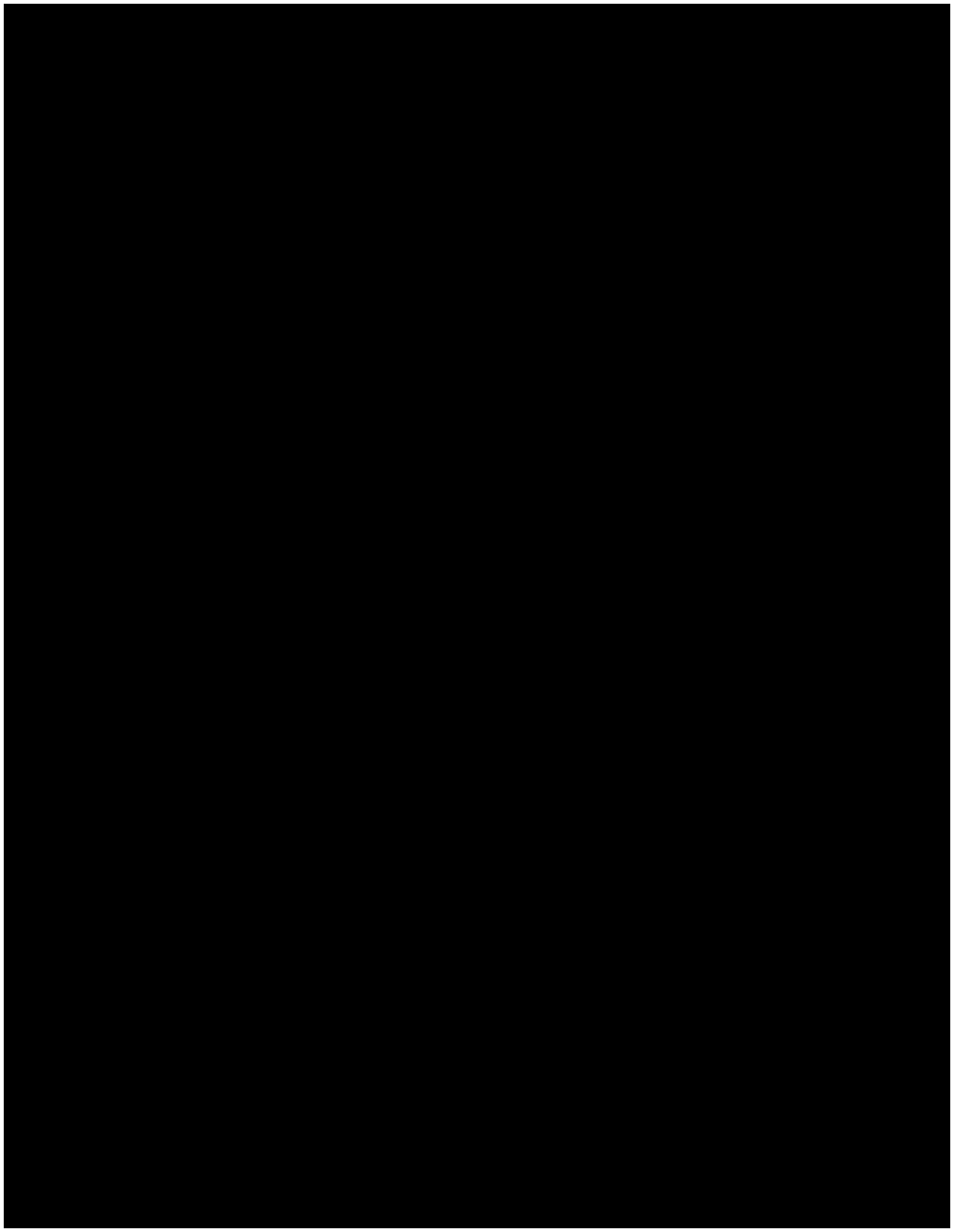


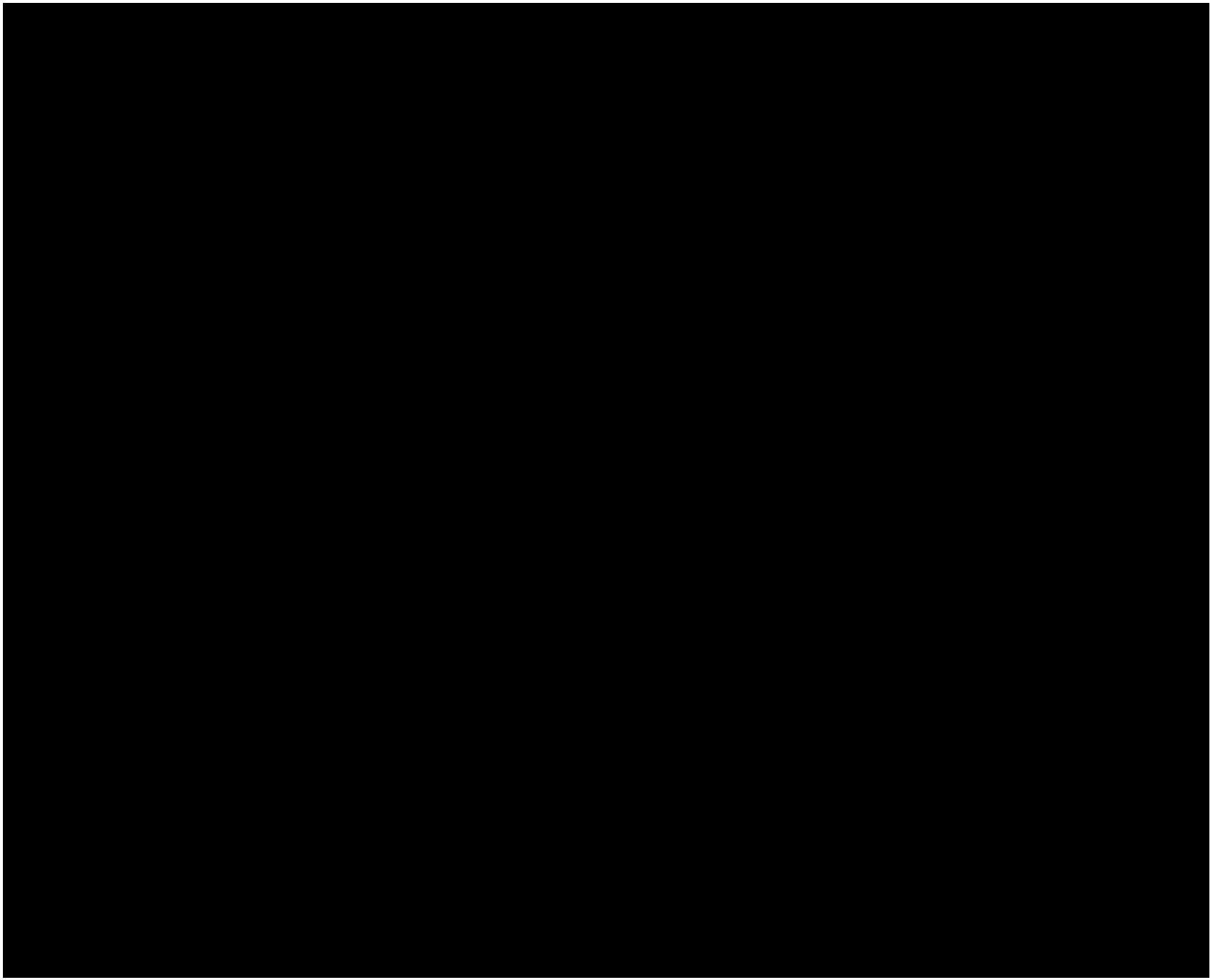


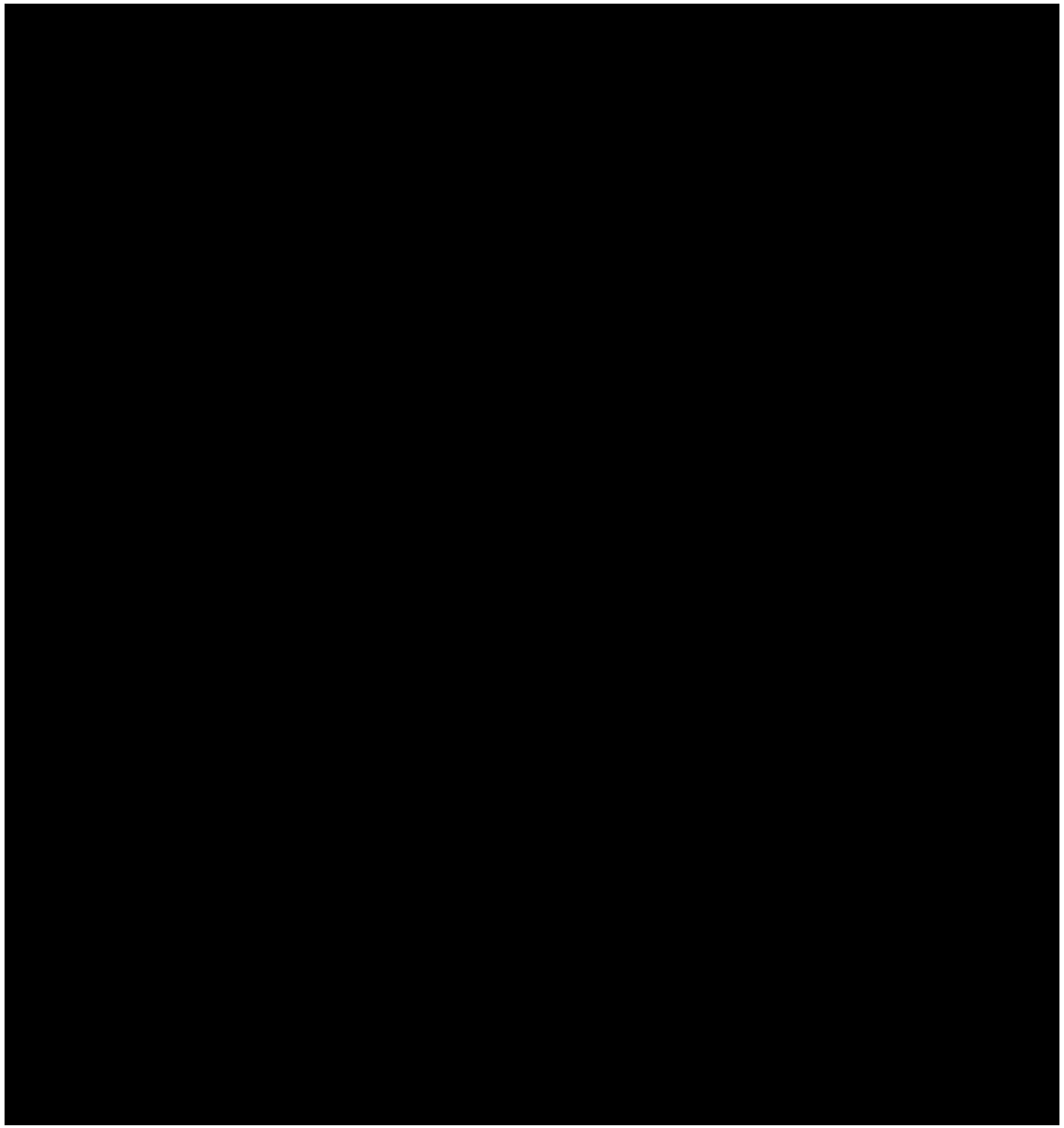


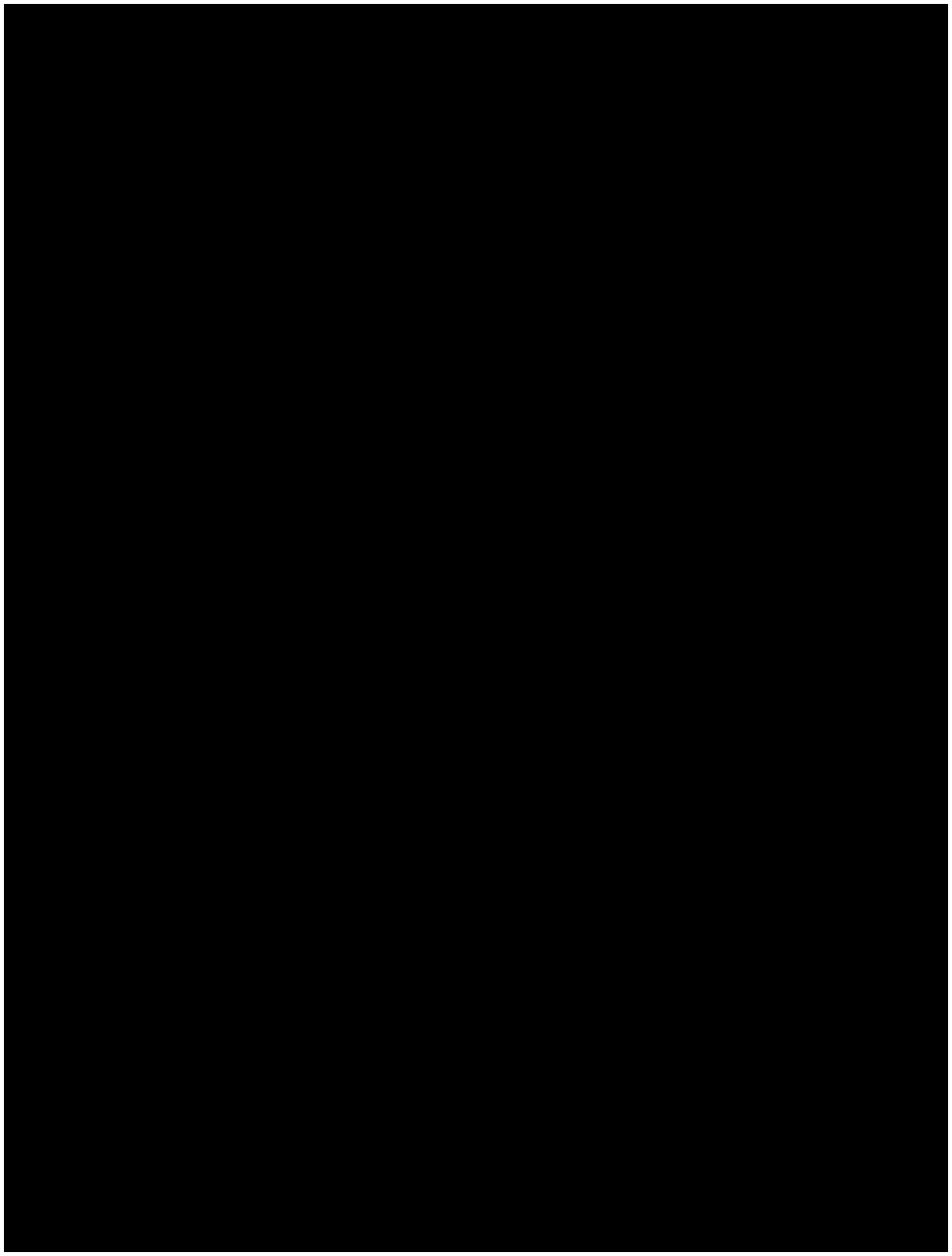


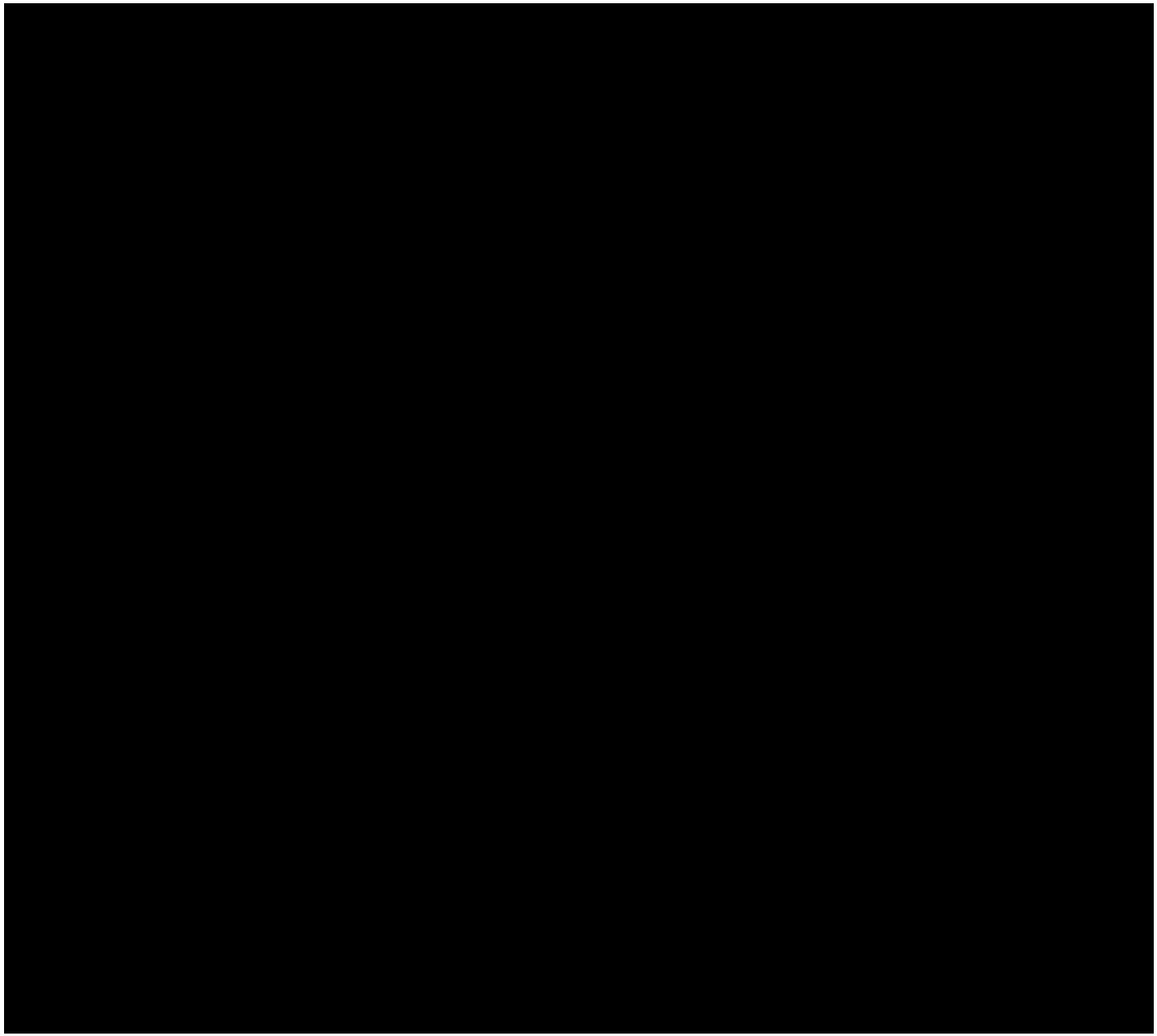


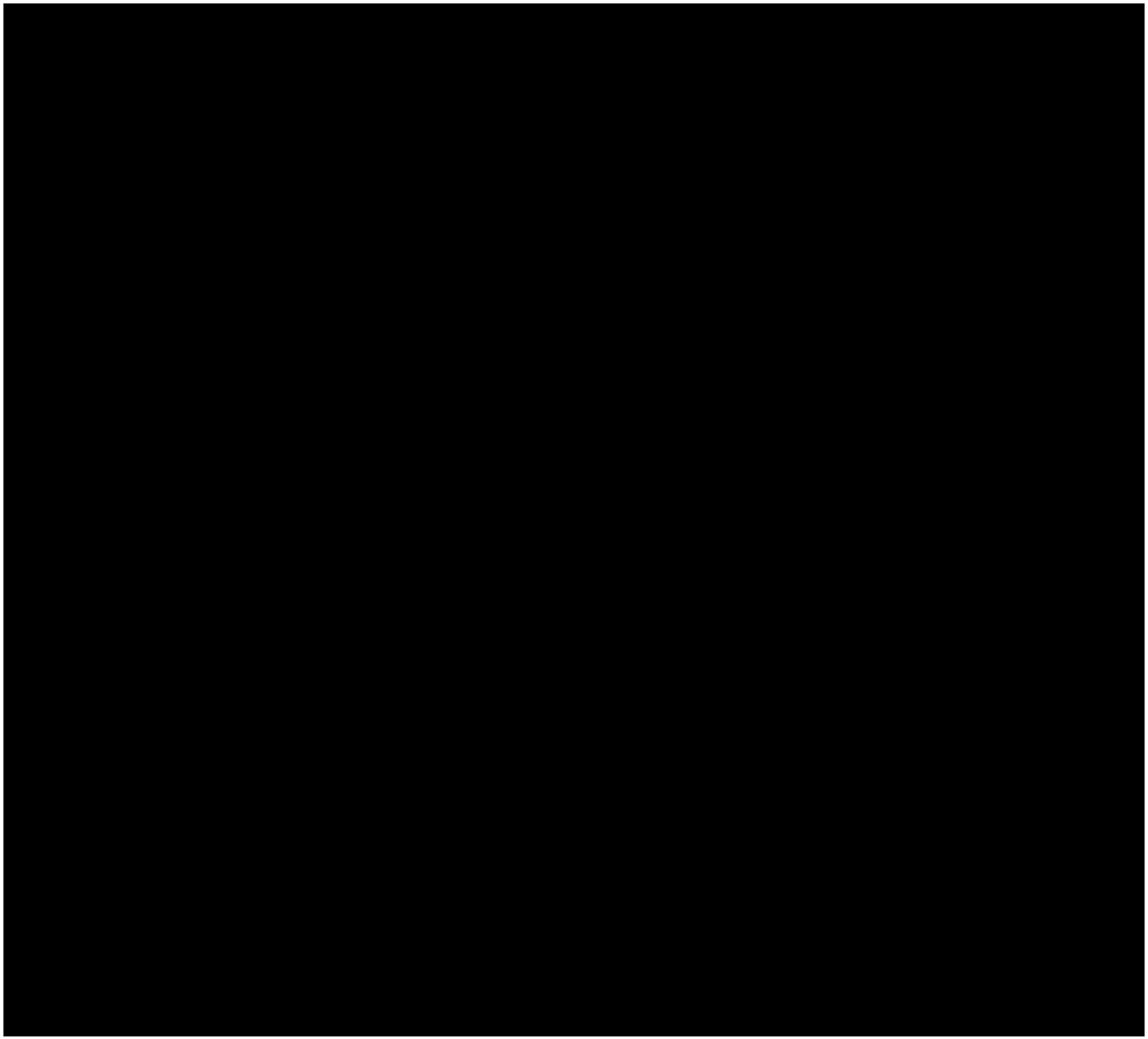


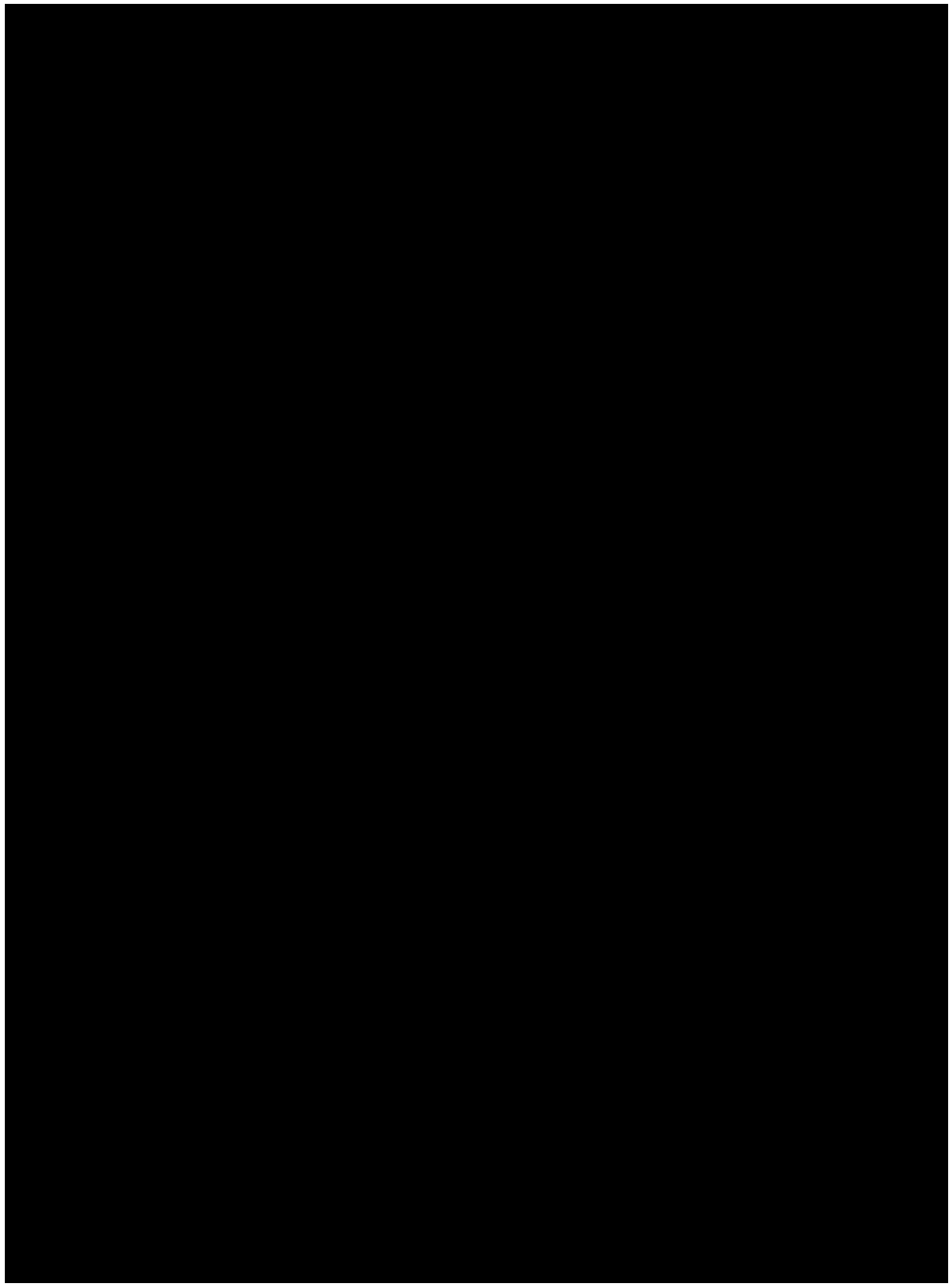


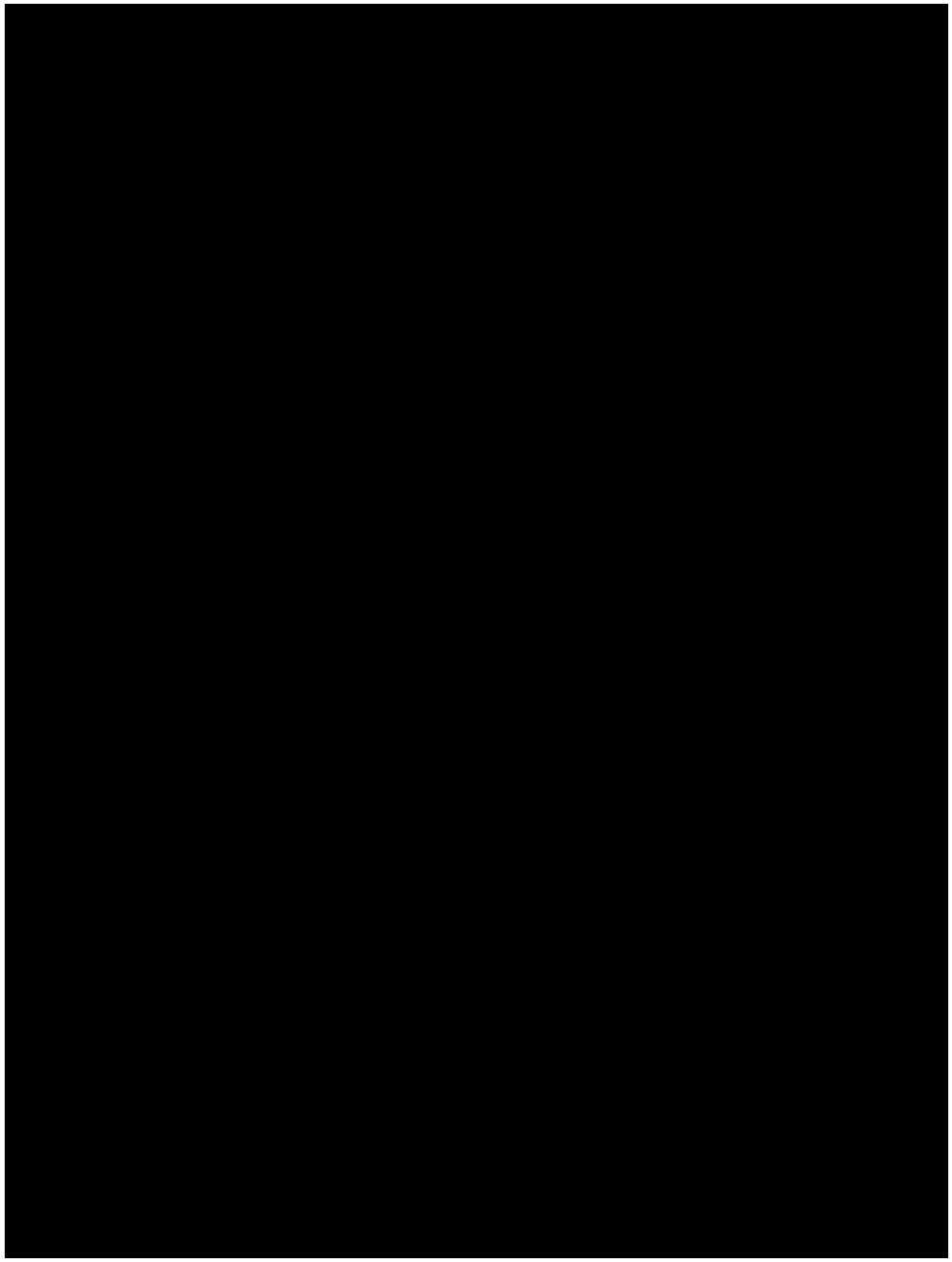


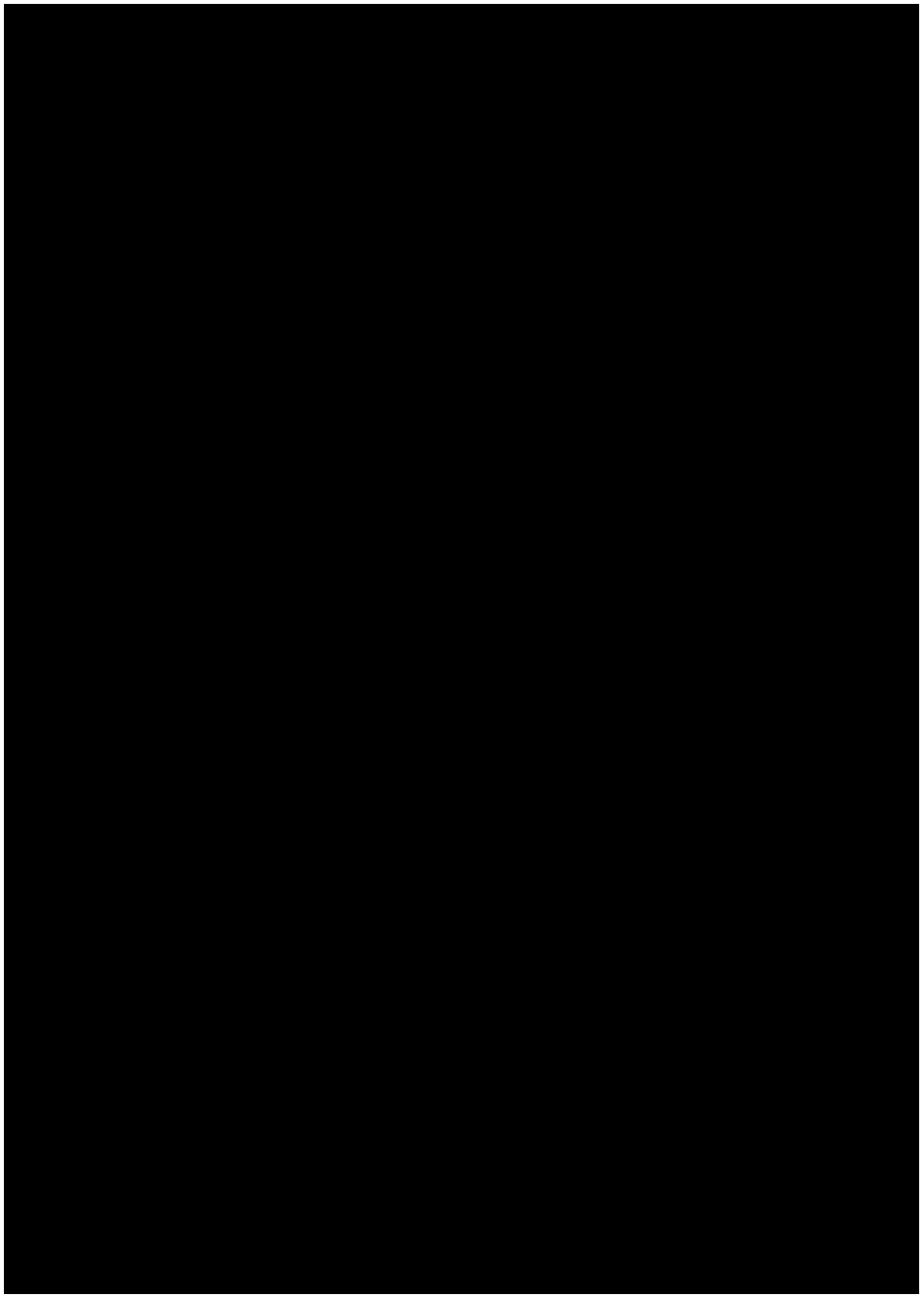


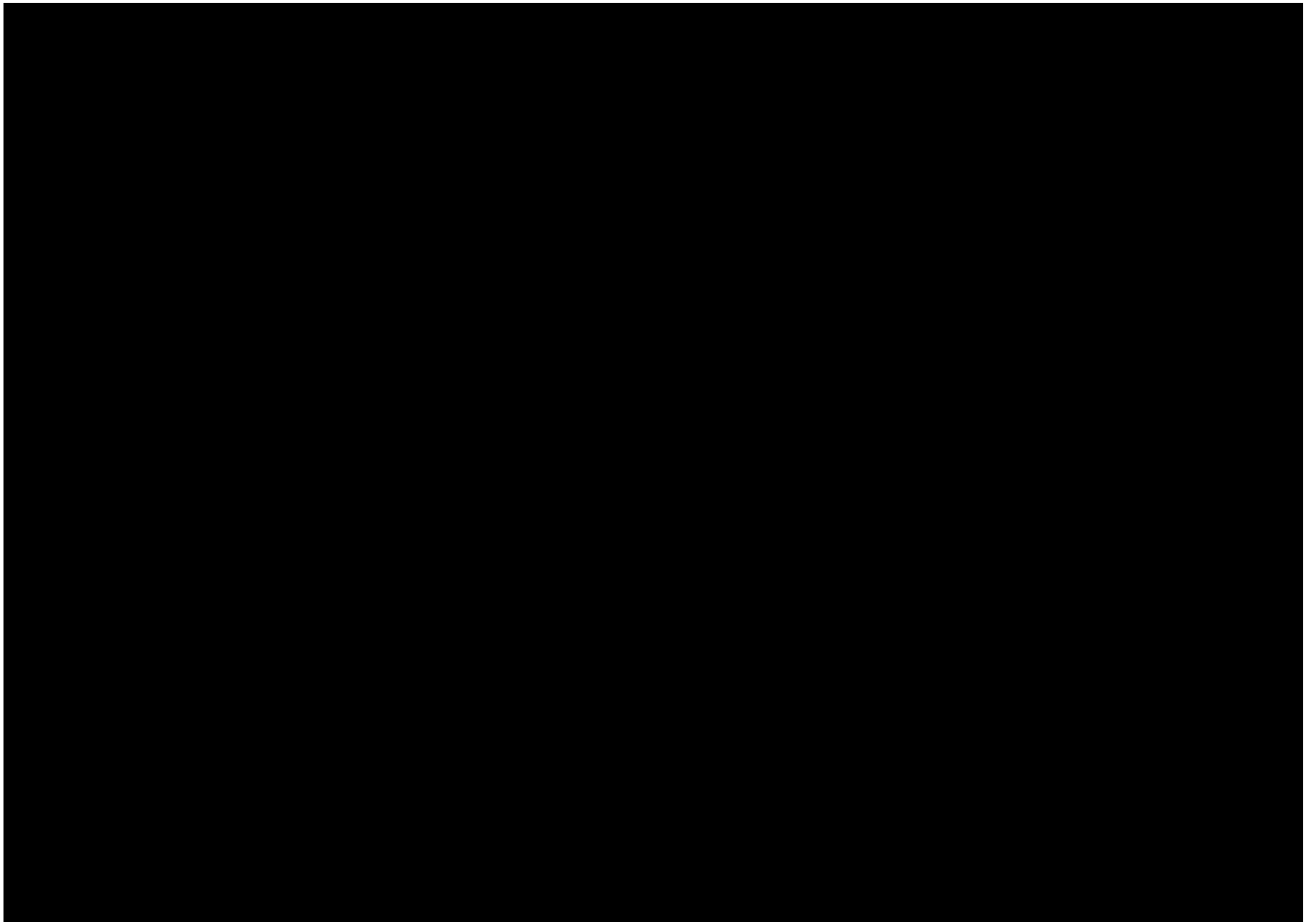


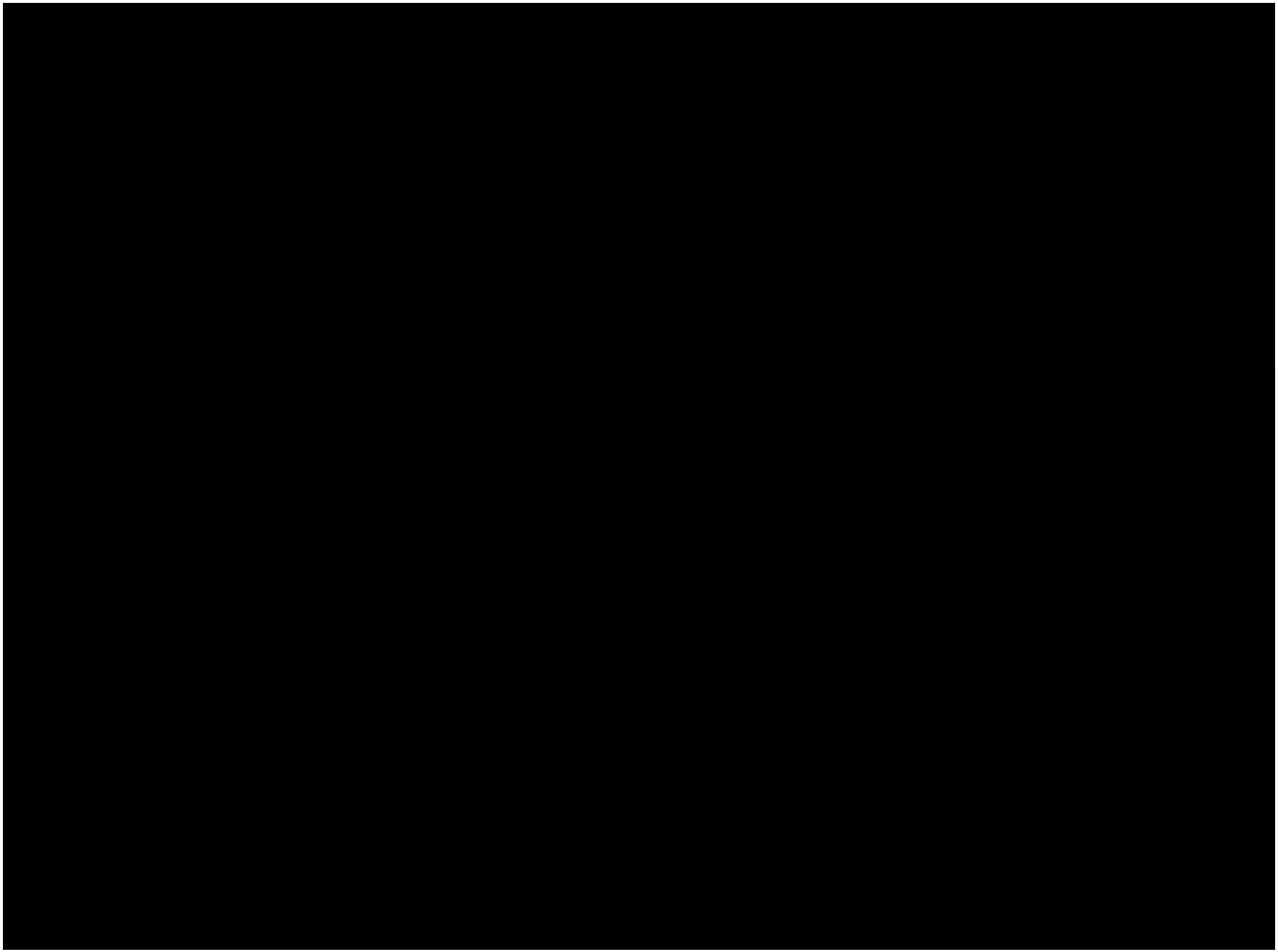


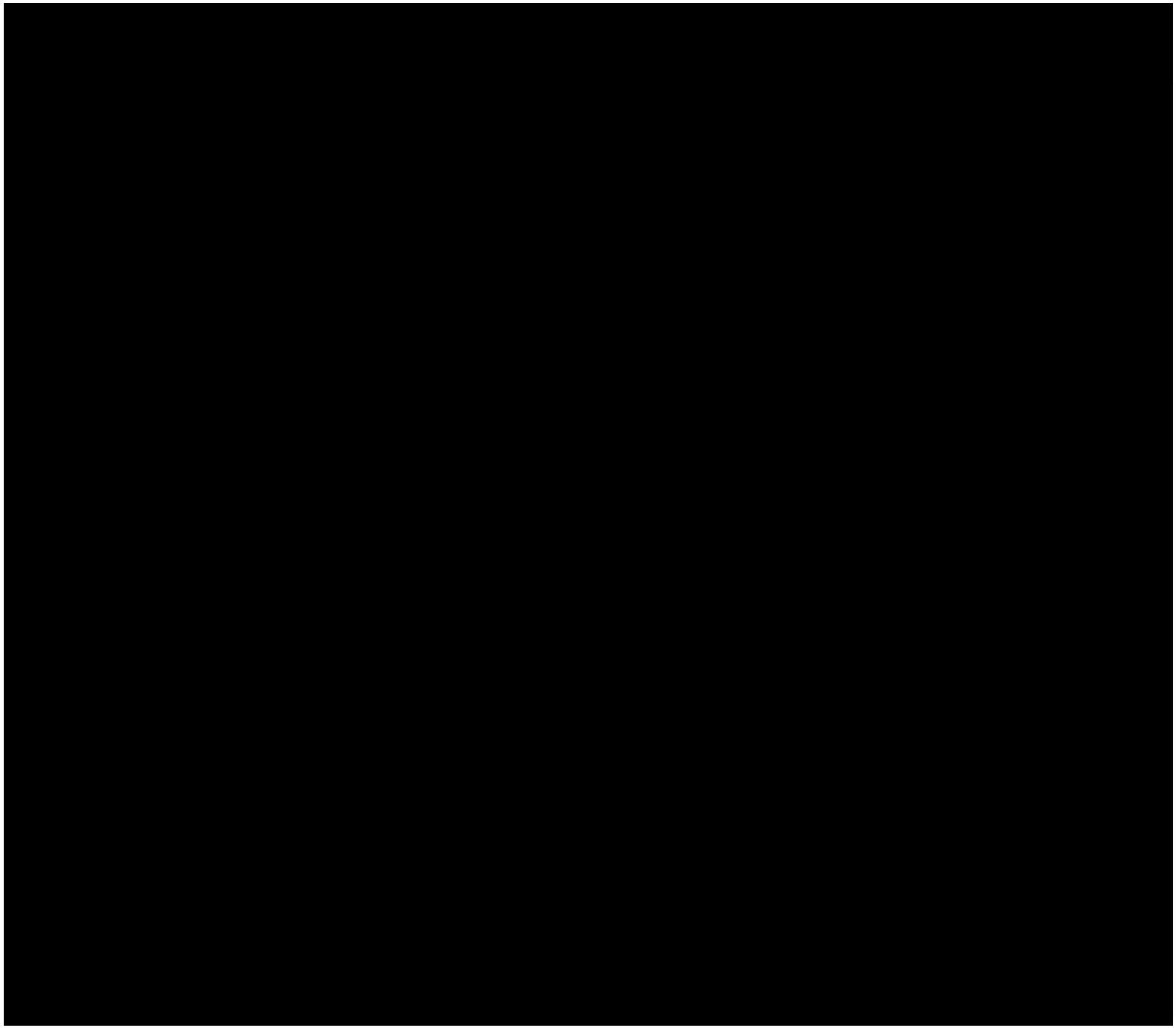


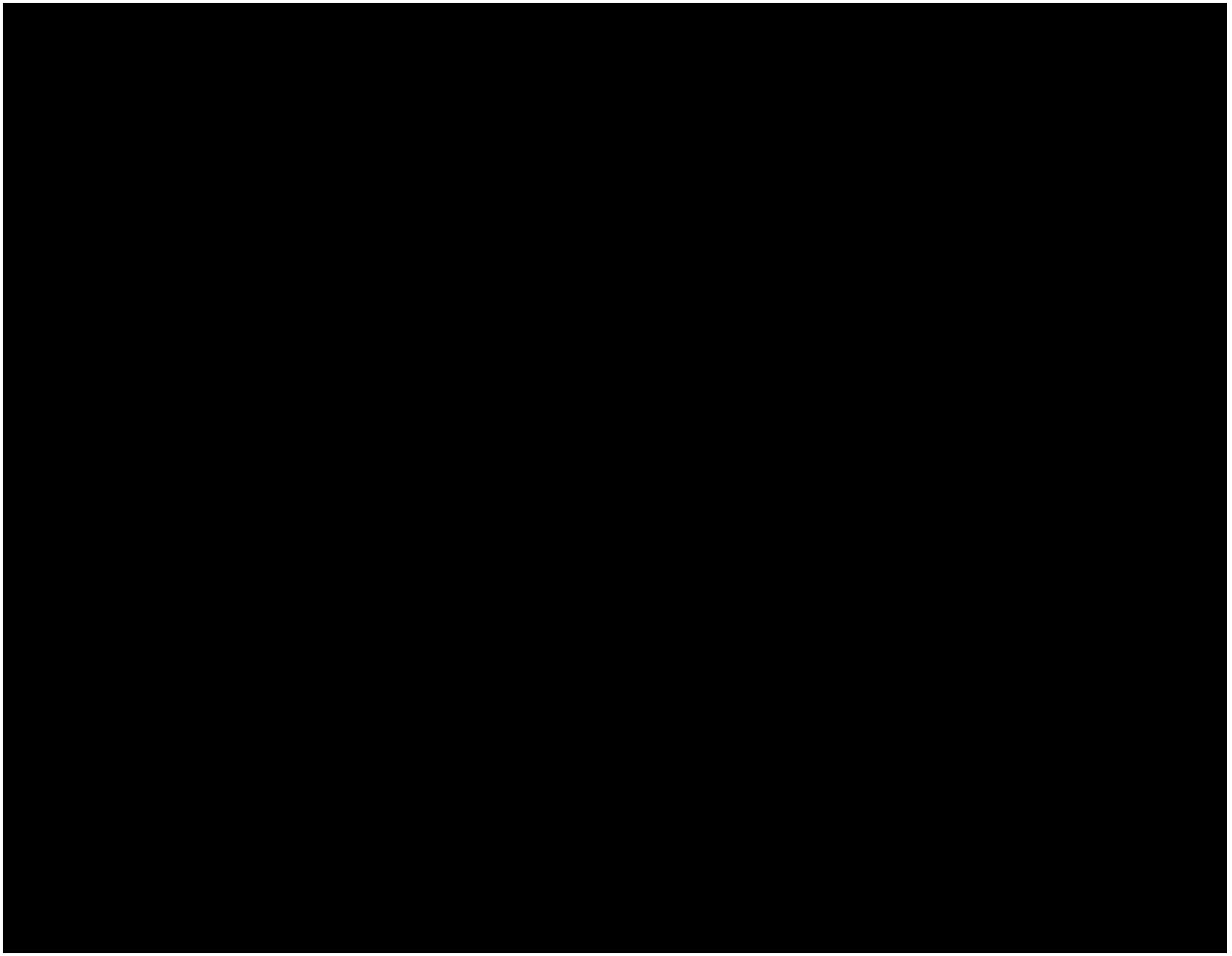












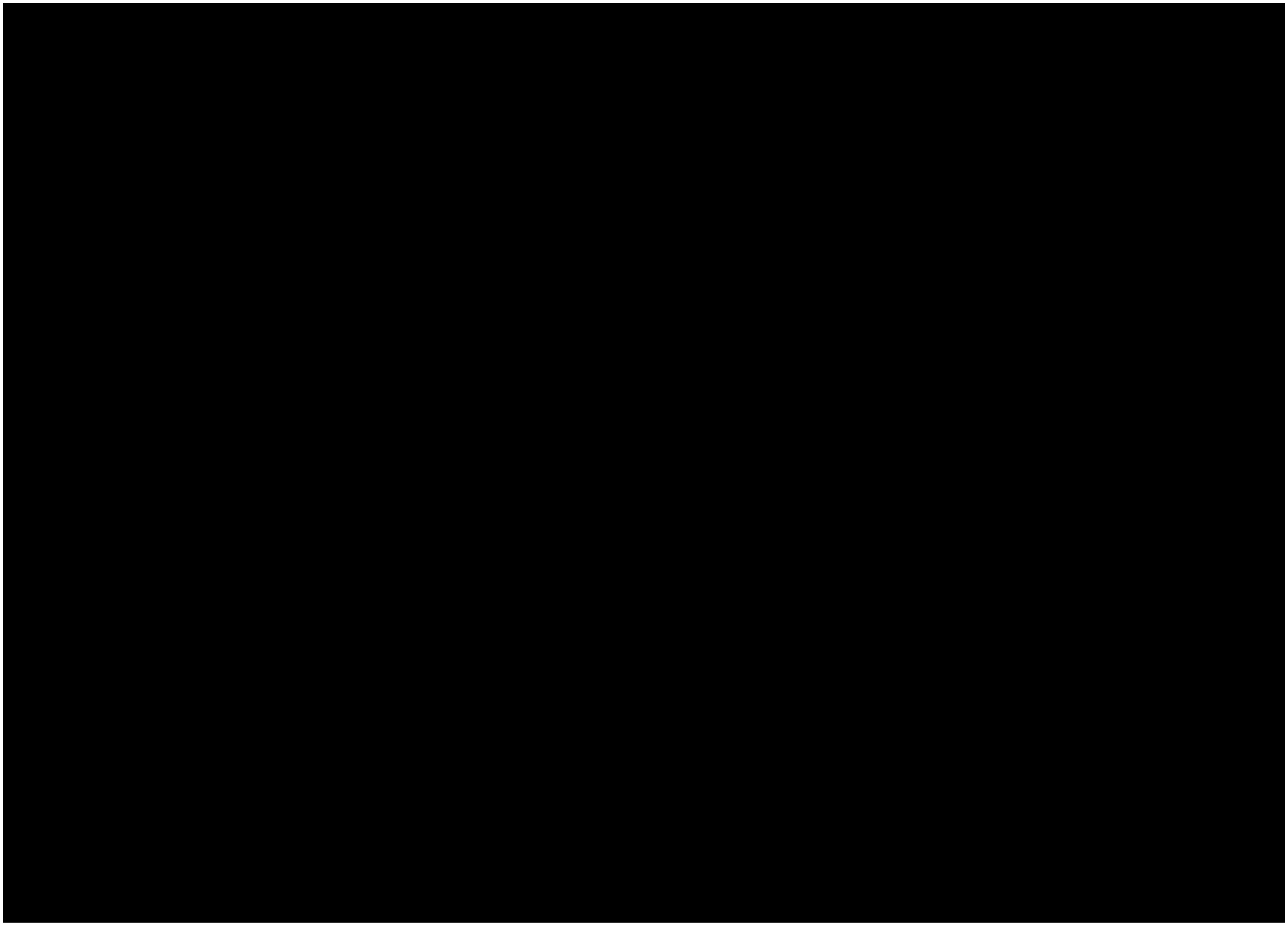


Exhibit 8

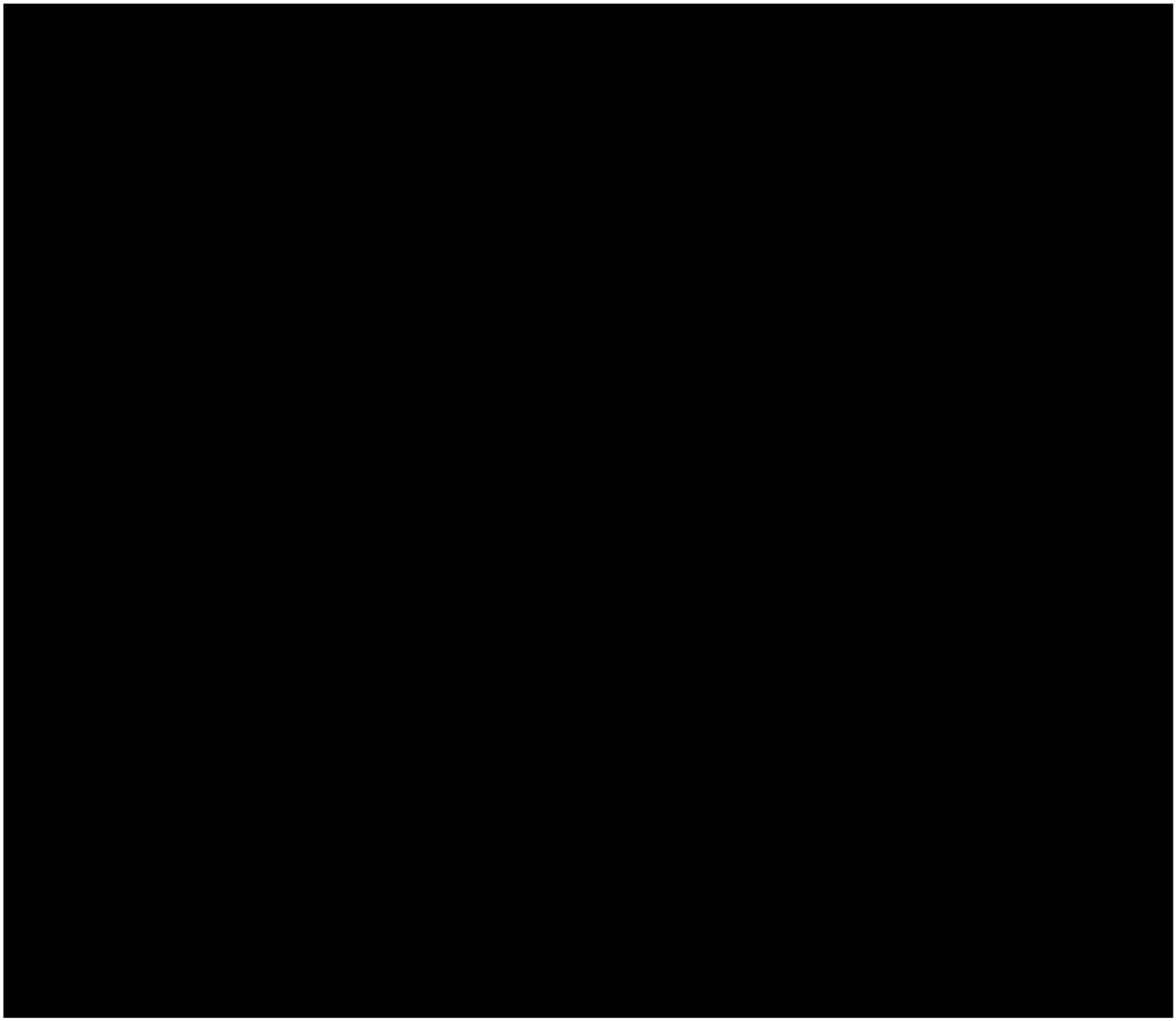
Tyler Indiana Incident Response Plan

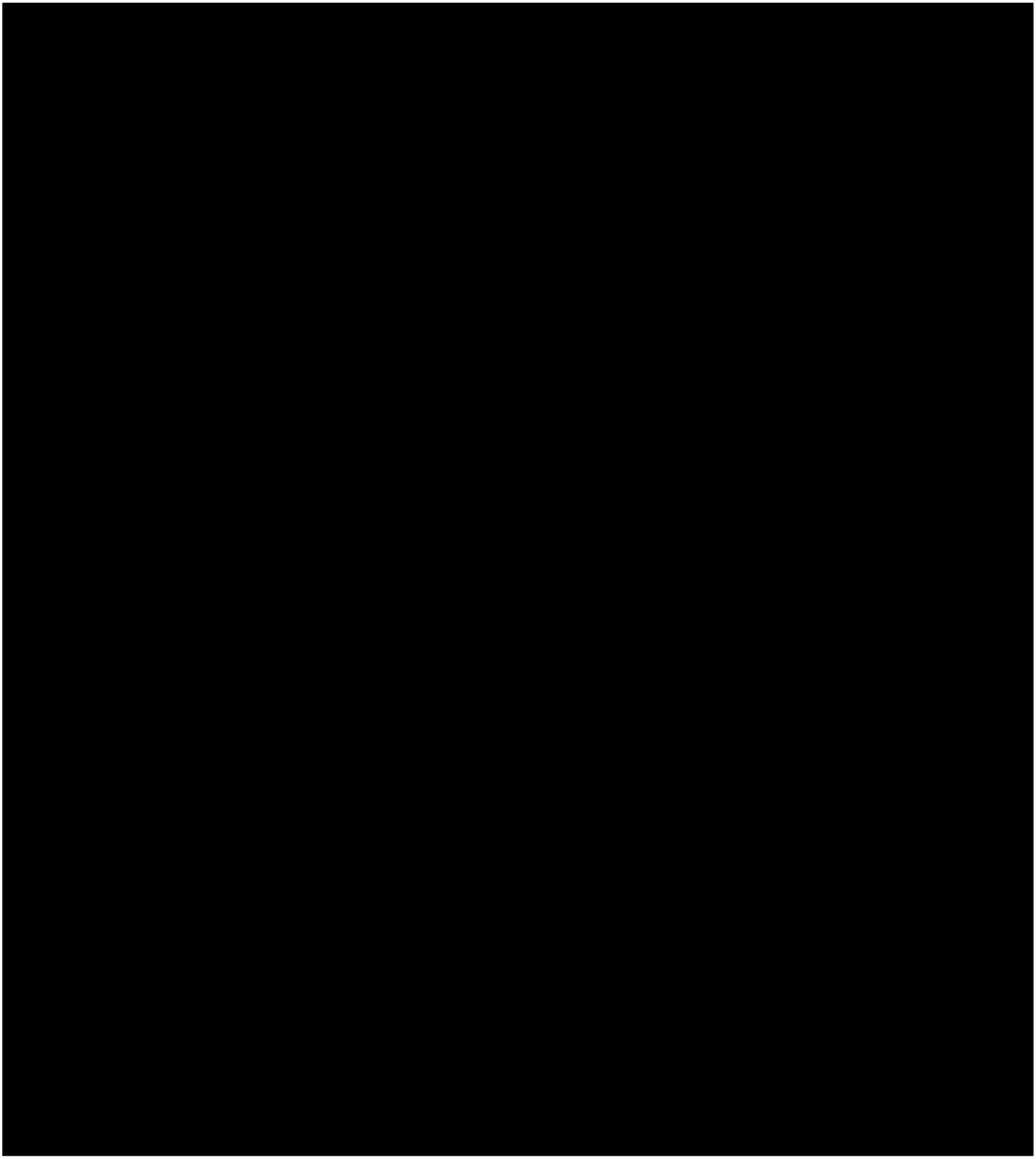
Version 2.0 August 22, 2023

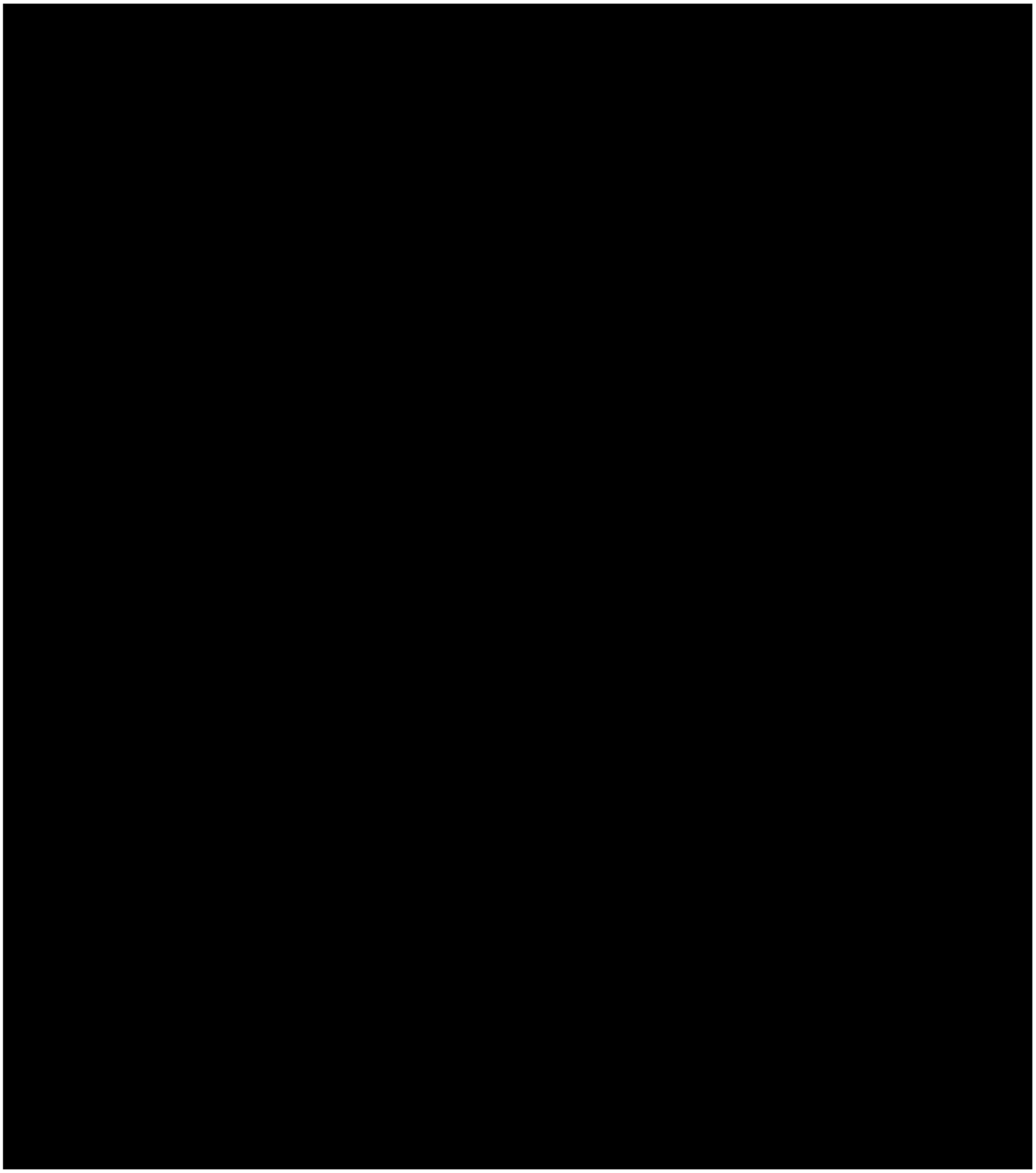
Tyler Indiana Response to RFP 23-74658

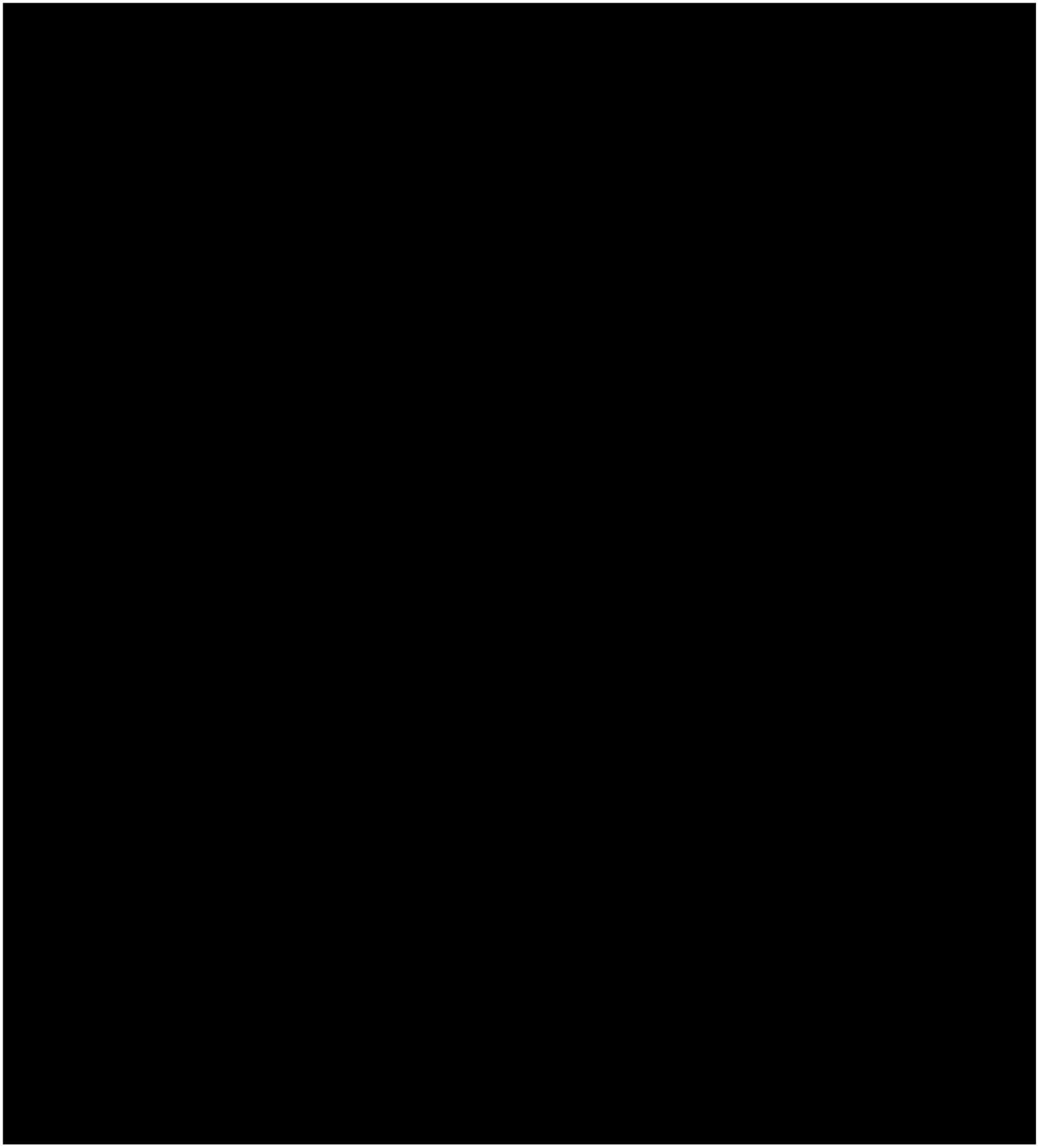
Attachment Name: F6 Privacy Incident Response Plan

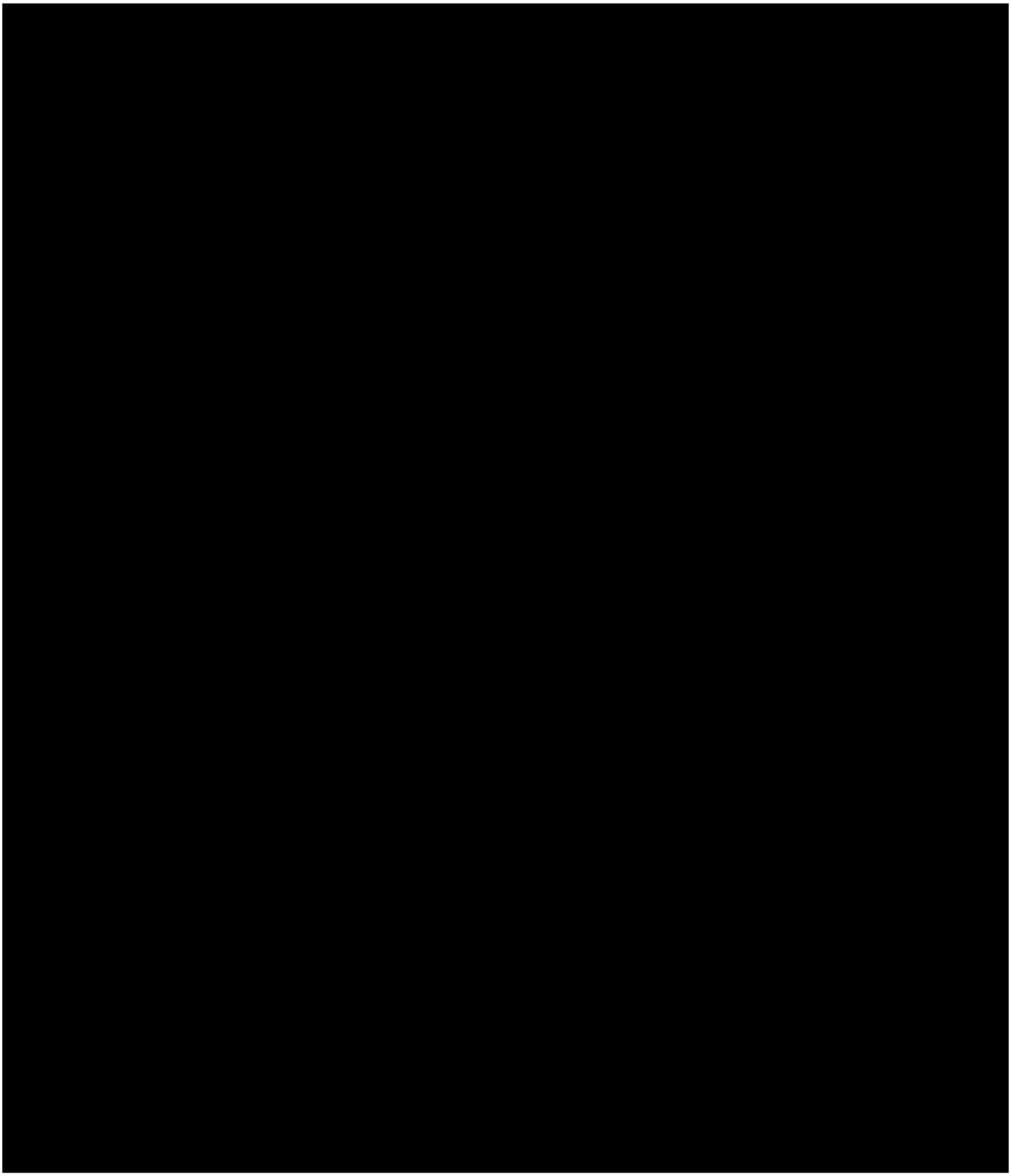
PROPRIETARY & CONFIDENTIAL

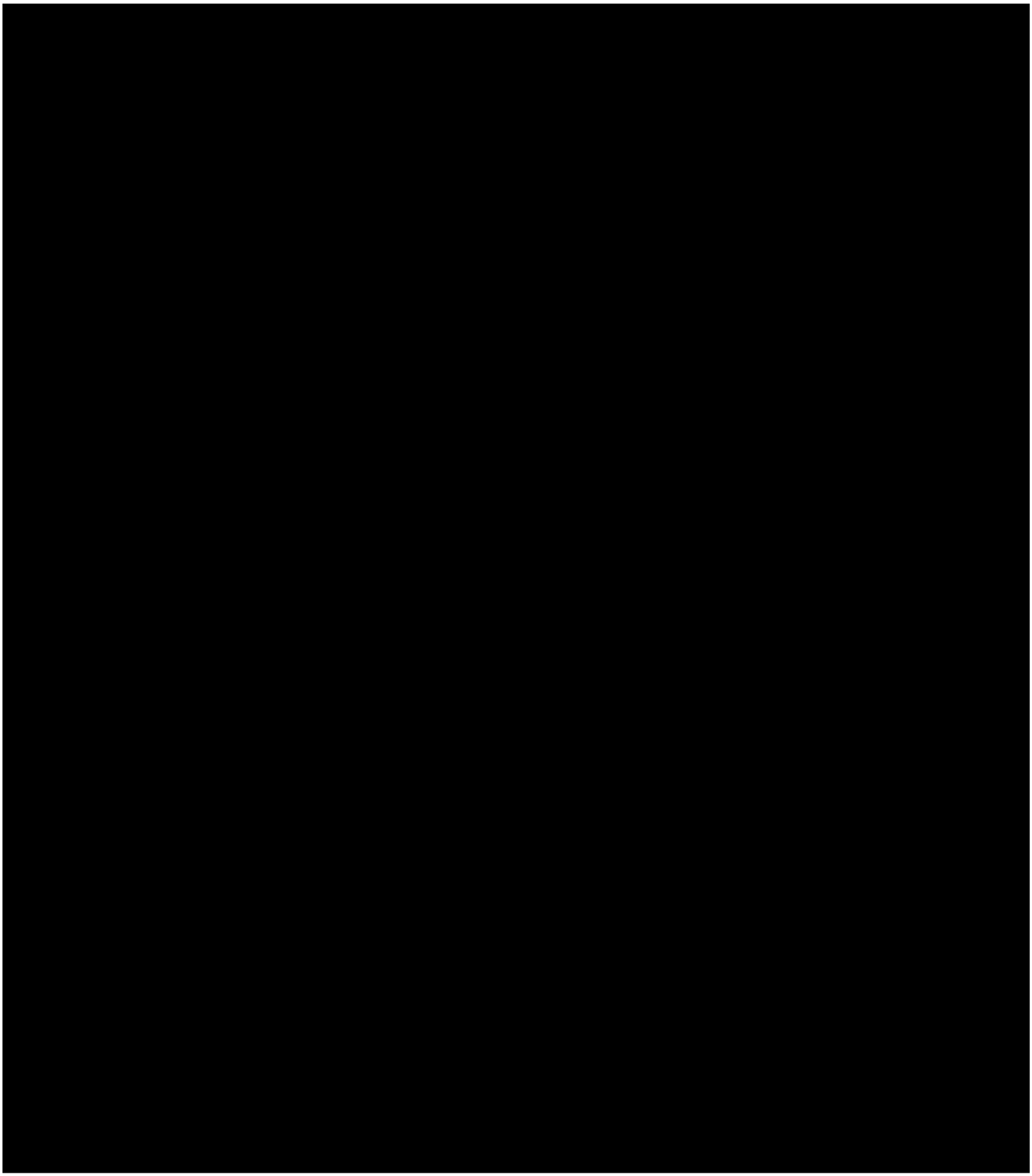


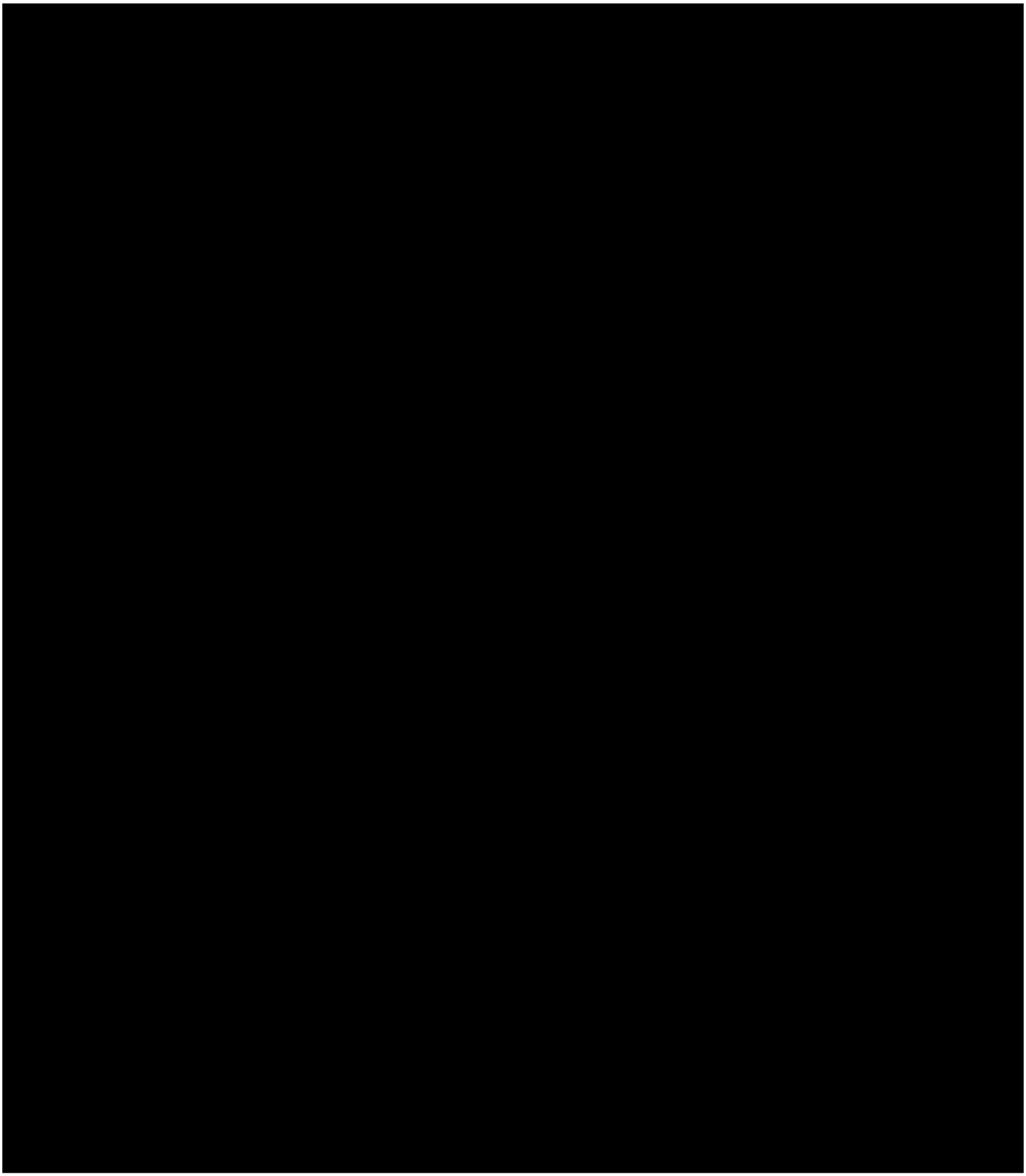


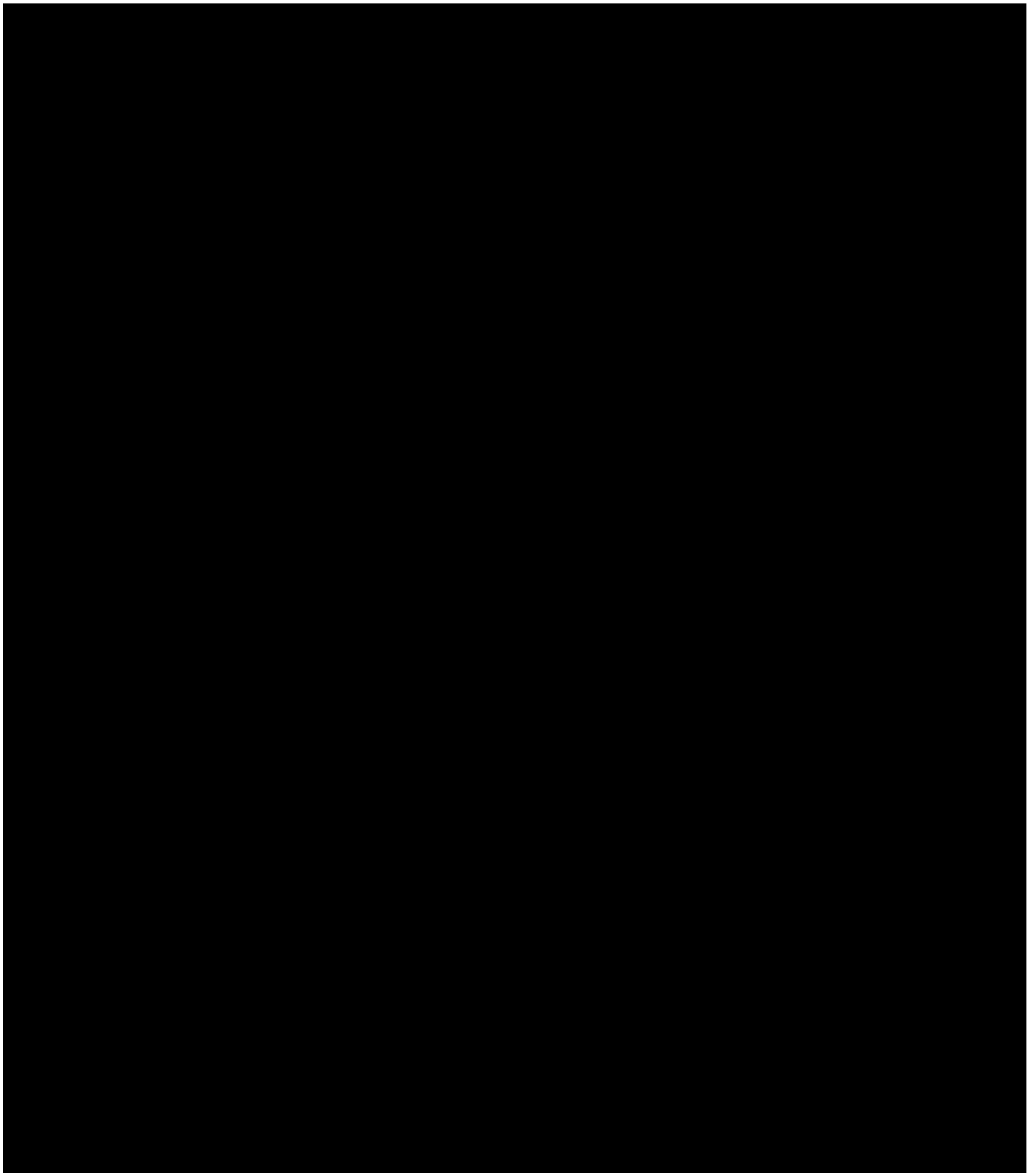


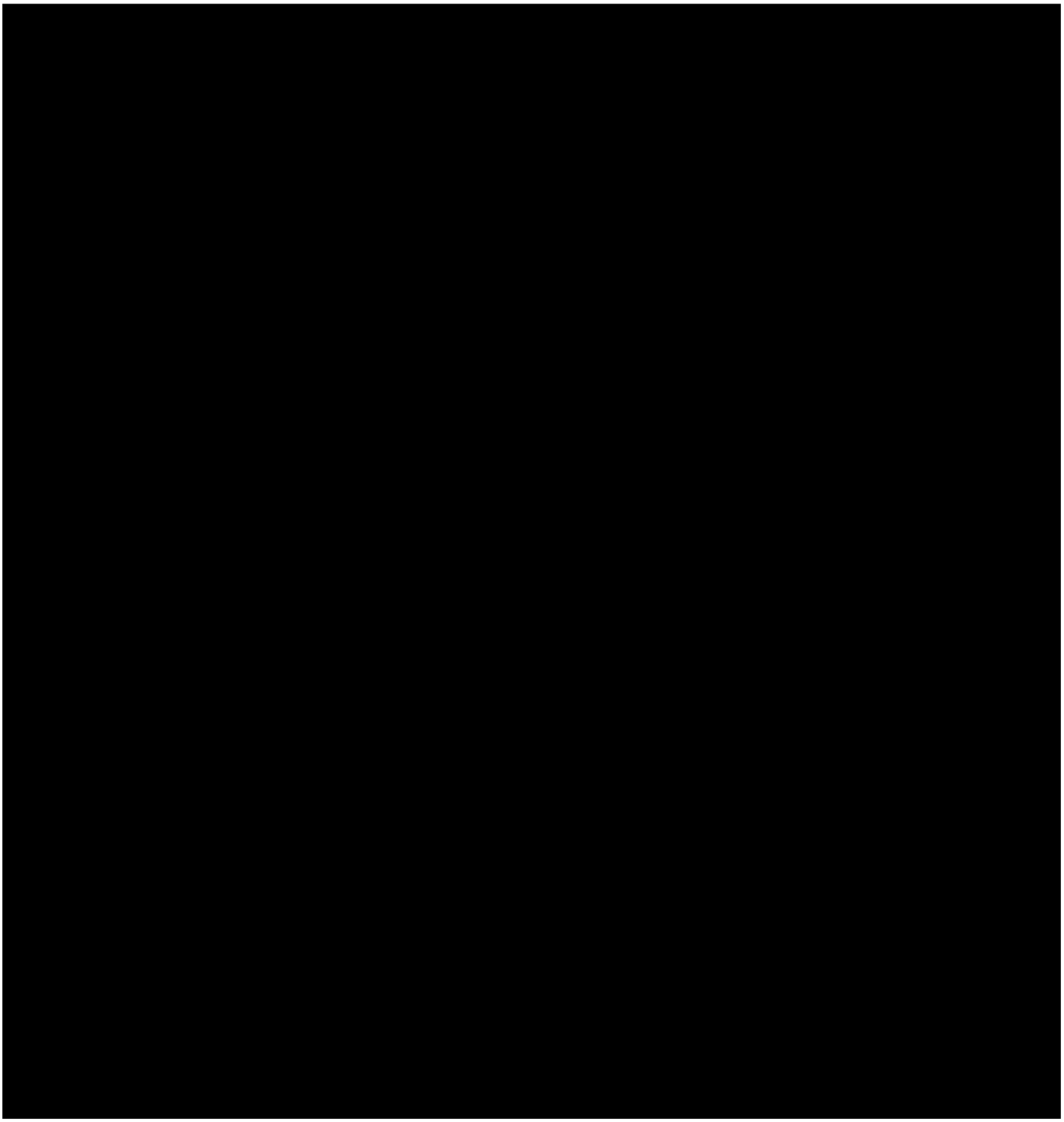












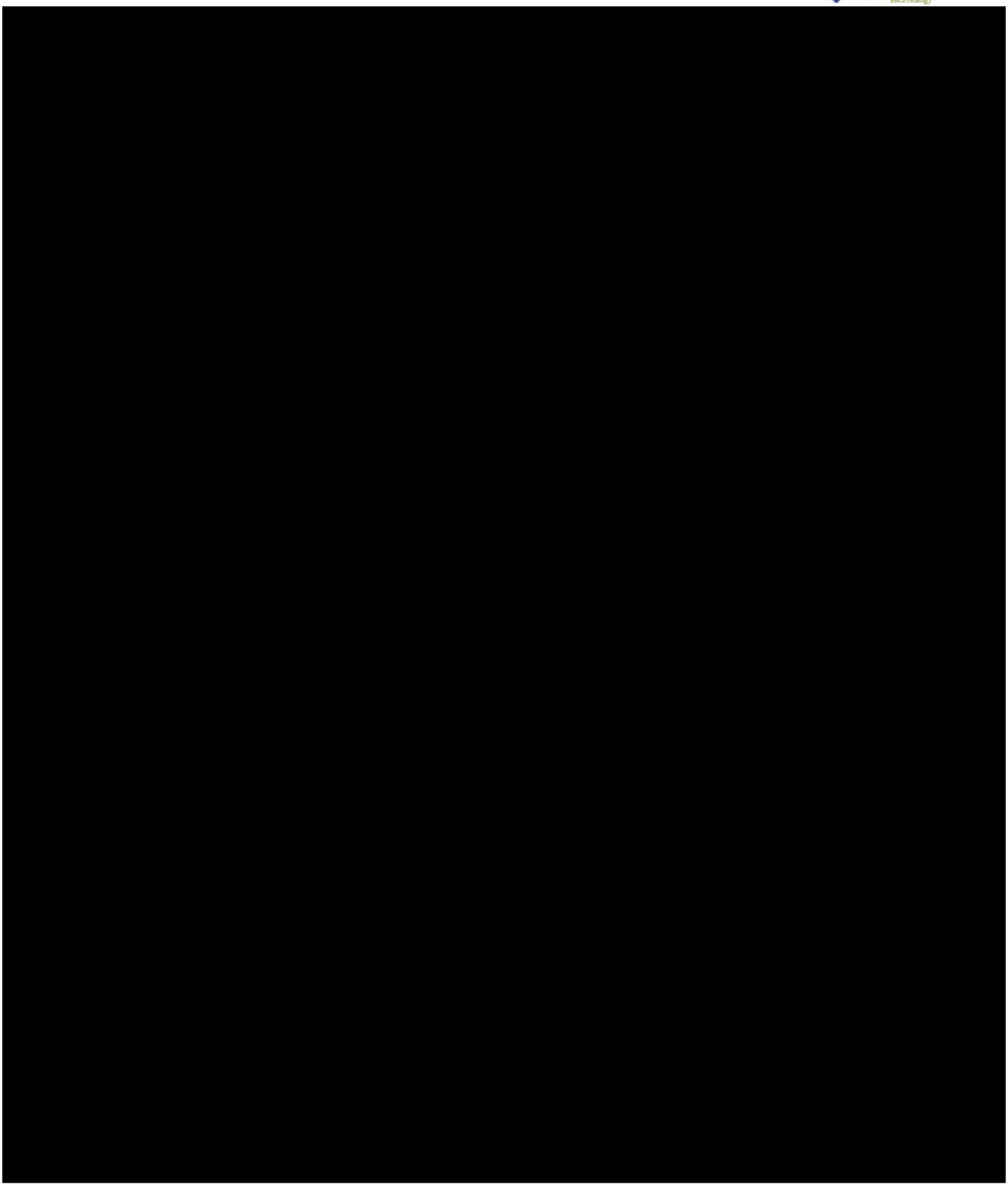


Exhibit 9
Staffing Plan

[redacted]

Exhibit 9

Staffing Plan

[redacted]

Exhibit 9

Staffing Plan

[redacted]

Exhibit 9
Staffing Plan

[redacted]

Exhibit 9

Staffing Plan

Exhibit 9

Staffing Plan

[redacted]

Exhibit 9

Staffing Plan

[redacted]

Exhibit 9
Staffing Plan

[redacted]

Exhibit 9

Staffing Plan

Exhibit 10

Organization Chart

[redacted]

[redacted]

Exhibit 11

Issue Priority Level Matrix

[redacted]

[redacted]