- Trade secrets; or
- Information that is commercial or financial, and that is obtained from a person and confidential or privileged.

2. Most of SSA's exemption 4 cases involve requests for materials submitted in connection with grants or contracts. Very little of this material comes under the trade secrets category.

B. **Trade Secrets**A trade secret is defined as a secret, commercially valuable plan, formula, process, or device that is used for the making, preparing, compounding, or processing of trade commodities and is the end product of either innovation or substantial effort. There must be a direct relationship between the trade secret and the productive process. Courts have recognized product manufacturing and design information as trade secrets, but not general information about a product's physical or performance characteristics.

C. **Commercial or Financial Information**
Almost any information relating to business or trade can be considered commercial or financial information. Records are commercial so long as the submitter has a commercial interest in them. Commercial includes anything pertaining or relating to or dealing with commerce. A non-profit entity can submit commercial information.

D. **Obtained from a Person**
The term "person" refers to a wide range of entities, including corporations and foreign governments. Information generated by the Federal government is not "obtained from a person" and is excluded from exemption 4 coverage. Information obtained from States also is generally excluded from coverage under exemption 4 unless it can be shown that the State is engaged in "commerce."

E. **Confidential Information**

1. **National Parks Test**

The courts established the two principal exemption 4 tests, known as prongs, for determining whether information is confidential in a case entitled, National Parks & Conservation Ass'n. v. Morton in 1974. Information is confidential if its disclosure would be likely to have either of the following effects:

- Impair the Government's ability to obtain necessary information in the future; or
- Cause substantial harm to the competitive position of the person from whom the information was obtained.
  - **Impairment Prong**
    The agency must determine whether businesses would continue to submit similar information if the information is disclosed.
  - **Competitive Harm Prong**
    he agency must determine whether disclosure would harm the competitive position of the submitter. The submitter must explain to the

agency in detail how disclosure of the requested material would result in significant harm to their competitive position or benefit their competitors.

2. **Analysis**
   - Answer the following questions in applying the National Parks test.
     - Does the submitter customarily hold this type of information in strict confidence and not disclose it to the public?
     - What is the general custom or usage of this type of information in the relevant occupation or business?
     - Who has access to the information? What types of individuals and how many?
     - What kind and degree of financial injury does the submitter expect if the information is disclosed?

F. **Designation of Confidential Information**

A person submitting records to the government may designate in writing part or all of the information as exempt from disclosure under FOIA exemption 4, either when submitting the records or within a reasonable time afterwards. A request for proposal (RFP) or request for quotation (RFQ) may require such a legend pursuant to 48 CFR 352.215-12. Any such designation will expire ten years after the records were submitted to the government.

G. **Submitter Notification**

Since the submitter of the information must make the case for withholding, SSA regulations provide that as soon as we receive a FOIA request for such materials, SSA will notify the submitter of the information about the request. We will ask the submitter to specify what material should be withheld and to explain in detail how disclosure of the re-quested material would significantly harm their competitive position or benefit their competitors.

H. **Examples of Exemption 4 Material**

The kind of information most often withheld under exemption 4 includes:

1. Technical data,
2. Cost data, including equipment and labor costs,
3. Wage schedules reflecting costs and overheads,
4. Profit margins,
5. Pricing and discount strategy, and
6. Names of key employees.

NOTE: This material is usually disclosed unless the submitter shows how disclosure will cause competitive harm.

14.12.10 Exemption 5 - Predecisional Information

A. **General**

Exemption 5 applies to "inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency." In other words, this exemption protects from disclosure those documents normally privileged, i.e., which could not be obtained in civil discovery by a private party engaged in a lawsuit with the agency. The three primary, most frequently invoked privileges that courts have held to be incorporated into exemption 5 are:

1. The deliberative process privilege,
2. The attorney work-product privilege, and
3. The attorney-client privilege.

B. **Threshold Requirement**

Exemption 5 applies only to documents of the kind intended to be covered by the phrase "inter agency or intra agency memorandums or letters." Although this phrase seems to refer only to documents generated by the agency itself, the courts have interpreted the phrase to include any document that is part of the deliberative process. Therefore, this exemption can apply in certain circumstances to documents generated by consultants outside an agency, and even to documents containing advice submitted voluntarily to an agency and for which the agency did not pay.

C. **Deliberative Process Privilege**

The deliberative privilege is the most frequently asserted privilege under exemption 5. This covers predecisional materials prepared as part of the decision making process in Federal agencies.

1. The purpose of this privilege is three-fold:
   - To encourage open, frank discussions on matters of policy among agency personnel;
   - To protect against premature disclosure of proposed policies before they are finally adopted, and
   - To protect against public confusion that might result from disclosure of rationale and reasons that were not in fact ultimately the grounds for an agency's actions.
2. To invoke the deliberative privilege the material in question must be both:
   - Predecisional (prepared before the agency adopted a policy), and

- Deliberative (makes recommendations or expresses opinions on legal or policy matters).
    - Drafts are very often exempt under this privilege; but even drafts, in order to be exempt, must be predecisional and related to a particular deliberative process.

3. Decisional and post decisional documents, which embody statements of policy and final opinions, are generally not exempt although they may be exempt to the extent they would disclose predecisional communications and elements of the decision making process.

4. Even if a document is clearly protected from disclosure by the deliberative process privilege, it may lose this protection if a final decision expressly incorporates it by reference. For example, an employee's recommendation which is adopted as policy may have to be disclosed if the policy is not restated elsewhere in another document.

5. This privilege generally does not apply to factual material. However, even the factual material in a document may be withheld if revealing the facts might also reveal the deliberative process. Since the writer is likely to incorporate only those facts that support a certain recommendation, disclosing which facts were selected could disclose the writer's mental process.

D. **Attorney Work-Product Privilege**

The second traditional privilege that exemption 5 incorporates is the attorney work product privilege, which protects documents prepared by an attorney in contemplation of litigation, setting forth the attorney's litigation strategy or theory of the case. The Supreme Court has held that documents qualifying as attorney work-products are entitled to perpetual exemption 5 protection. This privilege has a broad coverage in several respects.

1. Litigation need never have actually commenced, as long as the agency identifies specific claims that make litigation probable.

2. Non-attorneys may author documents constituting work-product, as long as they act under the general direction of attorneys.

3. Courts have held the work product privilege to persist even when the information has become the basis for a final agency decision.

4. The work-product privilege often permits agencies to withhold factual material because factual material may reveal the attorney's tactical and strategic thinking regarding litigation.

E. **Attorney-Client Privilege**

Exemption 5 also covers confidential communication between an attorney and his client relating to a legal matter for which the client has sought professional advice. The agency is the client, and SSA's attorney is usually the Office of the General Counsel. This

privilege does not hinge on the likelihood of litigation. It applies to facts divulged by the client to the attorney, and opinions given by an attorney to the client based on those facts. The client must have provided the information underlying the attorney's opinion, not other persons or sources.

F. **Other Privilege**
The courts have recognized another qualified privilege incorporated in exemption 5. Confidential research, development, or commercial information generated by the Government itself in the process leading up to the awarding of a contract may be protected if premature disclosure would significantly harm the Government's monetary function or commercial interests. This privilege expires when the agency awards the contract or withdraws the offer. An example of material falling into this category is Government prepared cost estimates used to evaluate proposals submitted in the competitive procurement process.

G. **Discretionary Exemption**
Exemption 5 is considered discretionary; that is, agencies do not have to withhold material just because it falls within the scope of exemption 5. From time to time, the Department of Justice issues guidance to agencies on when to invoke exemption 5, usually in the form of an Attorney General's Memorandum.

14.12.11 Exemption 6 - Personal Information

Exemption 6 permits agencies to withhold information about individuals in "personnel and medical files and similar files" if the disclosure would constitute a "clearly unwarranted invasion of personal privacy."

A. **Types of Records Covered**
It is generally easy to identify personnel and medical files. The term "similar files" is less clear. In 1982, the Supreme Court held that Congress intended a broad meaning of the term "similar files," and made clear that all information that applies to a particular individual qualifies for exemption 6 consideration.

B. **Privacy Interests**
The second step in analyzing exemption 6 material is assessing whether disclosure would invade a protectable privacy interest.

1. Some disclosures involve no invasion of privacy (e.g., duty stations of Federal employees).
2. Neither corporations nor associations have protectable privacy interests.
3. Deceased persons have no privacy rights. However, personal information about the deceased may involve the privacy rights of living individuals.

C. **The Balancing Test**

1. If an agency finds a privacy interest exists, it must balance the rights of the individual against any public interest in disclosure. There is no relationship between the planned use of the information and the public interest in disclosure.

    - The courts have always protected the personal, intimate details of a person's life. Exemption 6 protects information such as marital status, medical condition, welfare payments, criminal histories, and family reputations. Even the release of “favorable information," such as outstanding performance evaluations, may well cause embarrassment.

    - Agencies must balance the public interest, if any, in disclosure of the information against the privacy interest affected by disclosure. The only public interest agencies may consider is whether the information sought would improve public oversight and public accountability by giving the public an insight into an agency's performance of its statutory duties. The primary consideration in determining whether this public interest exists will frequently be the nature of the requested document. Agencies may not consider the identity of the requester, the requester's need for the information, or the requester's planned use of the information. A purely commercial purpose or a purely private matter, such as a lawsuit between two individuals, does not represent a public interest. Agencies must also consider the severity of the invasion of privacy, which must be, according to the FOIA, "clearly unwarranted.”

    - The courts have always accorded great weight in the balancing process to the public interest in disclosure of information about proven violations of the public trust (e.g., Federal employees found guilty of accepting bribes).

D. **Requests for Information about Federal Employees**

SSA frequently receives requests for information about Federal employees. Regulations of the Office of Personnel Management (OPM) provide for the release of name, position title and occupational series, grade, salary, duty station, position description, and identification of job elements. The Justice Department also recommends release of additional items, particularly those relating to professional qualifications. Personal details of an individual's Federal service are usually not disclosed (e.g., home addresses, names of disciplined employees, job performance evaluations).

E. **Release of Segregable Portions**

When we receive a request for records containing material falling under exemption 6, we should generally disclose all reasonably segregable non-exempt portions of the records. For example, we might release documents containing personal information if after deleting all identifying information no individuals could be identified. However, we may not be able to make the individuals unidentifiable if there are only a small number of individuals in the group, or if the request was for the records of identified individuals. For example, if a requester asks for the records of John Doe, we cannot make them unidentifiable by deleting his name.

14.12.12 Exemption 7 - Information Compiled for Law Enforcement Purposes

A. **General**

Exemption 7 protects "records or information compiled for law enforcement purposes." The use of the word "information" means that an item of information originally compiled by an agency for a law enforcement purpose does not lose Exemption 7 protection merely because it is maintained in or recompiled into a non-law enforcement record. In addition, an item of information initially compiled for a non law enforcement purpose may nevertheless qualify for Exemption 7 protection if it is subsequently recompiled for a valid law enforcement purpose. In other words, records generated pursuant to routine agency activities such as monitoring or oversight of government programs may qualify for exemption 7 protection if those activities involve a law enforcement purpose.

B. **Subpart A**

1. Exemption 7(A) permits the withholding of records or information compiled for law enforcement purposes if their disclosure could reasonably be expected to interfere with pending or prospective law enforcement proceedings. Possible intimidation of witnesses, discouragement of the involvement of witnesses, or the opportunity for a suspected violator to construct defenses constitutes interference with enforcement proceedings.

2. The second section of this subpart applies only to records withholdable under exemption 7(A) if the investigation or proceeding involves a possible violation of criminal law; and if there is reason to believe that the subject of the investigation or proceeding is not aware that it is pending; and if acknowledgment of the existence of the records could reasonably be expected to interfere with the enforcement proceedings. If all of these conditions are met, and only during the time they are all met, the requester will lawfully be advised that no records responsive to his or her FOIA request exist.

C. **Subpart B**

This subpart is primarily meant to protect individuals against pretrial publicity and is rarely used.

D. **Subpart C**

1. This subpart authorizes withholding if disclosure could reasonably be expected to constitute an unwarranted invasion of personal privacy, and is closely related to exemption 6. As in that exemption, which protects against a clearly unwarranted invasion of personal privacy, the public interest must be balanced against the privacy interest. However, the courts have implicitly recognized a public interest favoring the nondisclosure of personal privacy information, particularly the public interest in avoiding the impairment of ongoing and future law enforcement proceedings. In other words, the public interest may factor into both sides of the equation.

2. The courts have also recognized that the mention of an individual's name (even one who is not the subject of an investigation) in a law enforcement file carries a stigmatizing connotation. Therefore, this clause is frequently used to protect the identities of persons whose names appear in law enforcement files but who were never charged with any wrongdoing.

3. The identities of Federal, State and local law enforcement personnel mentioned in law enforcement files are routinely withheld under this clause, as may be the identities of individuals who provide information to law enforcement agencies.

4. This subpart cannot be used to deny a person information about himself or herself.

E. **Subpart D**

1. Exemption 7(D) provides two types of protection for confidential source information. The first clause protects, in any civil or criminal law enforcement records, the identity of a confidential source, but does not protect the information furnished by that source, unless the information itself would reveal the identity of the source (i.e., because it could have come from only one person). The identity of the informants is protected whether they provided information under an express promise of confidentiality or under circumstances from which such an assurance could reasonably be inferred.

2. Confidential sources include persons providing unsolicited allegations of misconduct, private institutions, foreign, State and local government agencies, and persons responding to inquiries from law enforcement agencies.

3. The second part of exemption 7(D) protects all information furnished by a confidential source to criminal law enforcement authorities in the course of a criminal investigation or to an agency conducting a lawful national security intelligence investigation. In contrast to the first clause of 7(D), the information is protected, whether or not it identifies the source.

F. **Subpart E**

Exemption 7(E) protects two categories of records and information involving law enforcement investigations or prosecutions. Under the first section of this subpart, techniques and procedures of law enforcement investigations or prosecutions may be withheld if they are not already well known to the general public. Under the second section, guidelines for law enforcement investigations or prosecutions may be withheld if disclosure would risk circumvention of the law.

G. **Subpart F**

Exemption 7(F) protects information compiled for law enforcement purposes that could reasonably be expected to endanger the life or physical safety of any individual.

14.12.13 Time Limits

A. **Decisions**

The FOIA requires each Federal agency to decide, within 20 working days after receiving a request for records, whether to comply with the request and immediately notify the person making the request of the determination and the reason therefore, and of the right of such person to appeal to the head of the agency any adverse determination. The 20 day period shall commence on the date on which the request is first received by the appropriate component of the agency, but in any event not later than ten days after the request is first received by any component of the agency that is designated in the agency's regulations to receive requests. The 20 day period shall not be tolled by the agency except that the agency may make one request to the requester for information and toll the 20 day period while it is awaiting such information that it has reasonably requested from the requester or if necessary to clarify with the requester issues regarding fee assessment. In either case, the agency's receipt of the requester's response to the agency's request for information or clarification ends the tolling period. When a requester who has been denied, appeals the decision, the FOIA requires the agency to decide within 20 working days whether to disclose the records.

B. **Filling Requests**

Agencies should fill requests for inspection and copying as soon as possible. If it is not possible to fill a request promptly see 14.12.14 A. above.

C. **Multitrack Processing**

The EFOIA amendments of 1996 authorize agencies that have difficulties in processing their FOIA requests within the FOIA guidelines to establish multitrack procedures. An agency that maintains two or more tracks must handle its requests on a first in, first out basis within each track. The intent is to give agencies the flexibility to respond to relatively simple FOIA requests more quickly through a multitrack system.
SSA has established three tracks.
Track 1 Cases that can be cleared very quickly; i.e., by getting a query only or that can be answered with material/information on hand.
Track 2 Cases that need material (for example, a case folder) from another component to complete. The material required does not need a substantive answer or decision on the request from the affected component.
Track 3 - Cases that require a substantive decision or input from the affected component (for example, contracts). These cases will usually take the longest time to process.

Each agency shall establish a system to assign an individualized tracking number for each request received that will take longer than 10 days to process and provide to each person making a request the tracking number assigned to the request. Each agency shall also establish a telephone line or Internet service that provides information about the status of a request to the person making the request using the assigned tracking number. Both systems shall include:

- the date on which the agency originally received the request; and
- an estimated due date on which the agency will complete action on the request.

14.12.14 Extensions of Time Limits

A. **General**

1. In unusual circumstances the time limits prescribed may be extended by written notice to the person making the request setting forth the unusual circumstances for such extension and the date on which a determination is expected to be dispatched. No such notice shall specify a date that would result in an extension for more than ten working days. If the request cannot be processed within the time limit, the agency shall notify the person making the request and provide the person an opportunity to limit the scope of the request so that it may be processed within the time limit or provide an opportunity to arrange with the agency an alternative time frame for processing the request or a modified request. To aid the requester, each agency shall make available its FOIA Public Liaison, who shall assist in the resolution of any disputes between the requester and the agency. Refusal by the person to reasonably modify the request or arrange such an alternative time frame shall be considered as a factor in determining whether exceptional circumstances exist. The agency may use an extension at either the initial or the appeal level, but not both. (The agency may use any balance of the 10 extension days not used on the initial request later at the appeal level.) FOIA authorizes extensions only if additional time is needed to:
    - Search for and collect requested records from field facilities or other establishments that are separate from the office processing the request.
    - Search for, collect, and appropriately examine a voluminous number of separate and distinct records which are included in a single request.
    - Consult with another agency having a substantial interest in the determination on the request or with two or more components of the agency having a substantial interest in the matter.

B. **Authority to Grant Extensions**

Only the Freedom of Information Officer and the Commissioner of Social Security (or his or her designee) has the authority to grant an extension of the time limits. The Freedom of Information Officer will notify the requester of the reason for the extension and when a final response may be expected.

C. **Failure to Meet Time Limits**

If the agency does not issue a decision on the request within the applicable time limits, a member of the public may deem his or her request denied and seek court assistance in obtaining the requested records. Further, an agency shall not assess search fees (or in the case of educational and scientific institutions or news media, duplication fees) if the agency fails to comply with any time limit, if no unusual or exceptional circumstances apply to the processing of the request.

14.12.15 Requests for Expedited Processing

A. **Compelling Need**

The 1996 amendments to the Freedom of Information Act (E FOIA amendments) require agencies to promulgate regulations providing for expedited processing of requests for records where the requester demonstrates a "compelling need" as defined by the statute or in any other case the agency determines appropriate under its regulations. 5 U.S.C. 552(a)(6)(E). SSA's implementing regulation (20 CFR § 402.140(d)) defines "compelling need" as one of the following situations:

1. **Threat to life or safety**

   Failure to obtain the records quickly could reasonably be expected to pose an imminent threat to the life or physical safety of an individual.

2. **Media request for urgent news**

   The requester is a person primarily engaged in disseminating information and can demonstrate that there is an urgency to inform the public concerning actual or alleged Federal Government activity.

3. **Loss of legal right or benefit**

   The requester may be denied a legal right, benefit, or remedy without the requested information, and it cannot be obtained elsewhere in a reasonable amount of time.

B. **Time Limits**

Agencies must make a decision on a request for expedited access within 10 calendar days of receipt by the proper FOIA office and notify the requester. If we grant a request for expedited processing, the requester should be notified as soon as practicable of the agency's decision as to whether or not the records requested will be disclosed.

C. **Appeal Rights**

1. **Administrative Review**

   A requester can administratively appeal a denial of a request for expedited processing. Agencies must decide appeals expeditiously.

2. **Judicial Review**

   A requester can seek judicial review if the agency fails to decide an appeal in a timely manner. Judicial review shall be based on the record before the agency at the time of the determination. A U.S. district court does not have jurisdiction to review an agency denial of expedited processing after the agency has provided a complete response to the request.

14.12.16 Sanctions

A. **No Monetary Damages**
FOIA does not authorize any award of monetary damages to a requester, either for unjustified refusal to release requested records or for allegedly improper disclosure.

B. **Disciplinary Action**

1. Agency employees who act arbitrarily and capriciously in withholding information may be subject to disciplinary action. Specifically, subsection (a)(4)(F) of the FOIA provides that when a court
    - Orders production of improperly withheld agency re-cords, and
    - Assesses against the Government reasonable attorney fees and litigation costs, and
    - Issues a written finding that the circumstances surrounding withholding raise questions whether agency personnel acted arbitrarily or capriciously with respect to the withholding, the U.S. Office of Special Counsel will determine whether disciplinary action is warranted against the officer or employee who was primarily responsible for the withholding.

2. In most SSA FOIA cases, the employee primarily responsible for withholding information would be the SSA Freedom of Information Officer. However, any SSA employee who refuses to release records to the Freedom of Information Officer for a decision on disclosure thereby becomes the employee primarily responsible for withholding the information.

14.12.17 Authority

This Instruction is issued in accordance with the applicable provisions of 5 U.S.C. 552 and the SSA Regulation on Availability of Information and Records to the Public (20 CFR Part 402).

Freedom of Information Act Responsibilities of SSA Officials

Manual/Chapter: General Administration » Disclosure/Confidentiality of Information
Instruction/Handbook: GAM 14.13
Audience: General
Level: SSA
Inquiries: Office of Privacy and Disclosure (OPD) | [redacted]@ssa.gov | 410-966-6645
Related Instructions: Office Of The General Counsel (OGC) » Office of Privacy and Disclosure (OPD)
Updated: 7/17/2020
Certified: *(not yet certified)*

Table of Contents

14.13.01 Purpose

This Instruction describes the duties and responsibilities of SSA officials in complying with the Freedom of Information Act (FOIA), and the delegations of authority to release or withhold records requested by members of the public.

14.13.02 General

A. The FOIA requires Federal agencies to:

1. Publish certain materials in the Federal Register,
2. Index certain instructional materials,
3. Make certain materials available to the public for inspection and copying,
4. Disclose records on request, with certain specified exceptions, to members of the public,
5. Comply with time limits for responding to requests for records,
6. Establish a schedule of fees to be charged when members of the public request records,
7. Report annually to the Attorney General on FOIA activities, and
8. Prepare a FOIA reference guide describing major information systems and FOIA processes to aid potential FOIA requesters and post it on the Agency web site.

   AIMS, GAM 14.12 describes these requirements.

B. The National Archives and Records Administration (NARA) has established a retention schedule for records of FOIA requests. See AIMS, GAM 14.13.11 below.

14.13.03 SSA Freedom of Information Officer

The Deputy Executive Director, Office of Privacy and Disclosure (OPD), Office of the General Counsel is the SSA Freedom of Information (FOI) Officer. Only the Director, OPD, or his or her designee, may determine whether to release or withhold SSA records, including records in field offices and installations, in response to FOIA requests, except as otherwise provided by regulation. See AIMS, GAM 14.13.08 for requests that require action by the FOI Officer.

14.13.04 Responsibilities

A. **SSA Freedom of Information Officer**
The SSA Freedom of Information Officer is responsible for:

1. Providing policy guidance, technical assistance, and general oversight for compliance with the FOIA.

2. Directing the development of policies and assisting in the development of regulations for implementing FOIA provisions.

3. Serving as the focal point for SSA FOIA activities and as the primary liaison with other agencies on FOIA matters.

4. Maintaining SSA's Index of Administrative Staff Manuals and Instructions (IASMI).

5. Maintaining the FOIA Reading Room on SSA's web page.

6. Reviewing all proposed replies drafted by other components to requests for SSA records from members of the public (excluding Privacy Act requests or disclosures provided for by regulations) and deciding whether the requested records should be released or denied.

7. Coordinating responses to requests for records maintained in two or more SSA offices and coordinating responses and clearances on appeals of FOIA denials.

8. Reviewing requests for waiver of fees for copies of SSA records and instructional materials and deciding whether the fee should be waived, and replying to these requests.

9. Collecting data from SSA components and preparing the SSA Report to the Attorney General on FOIA activities.

10. Providing technical assistance for development of training of SSA staff on FOIA provisions and requirements.

B. **Commissioner and General Counsel**
Any person whose request has been denied may request a review by the head of the Agency or his/her designee. The Commissioner has delegated authority to review appeals of FOIA denials to the General Counsel, who in turn redelegated this authority to the Executive Director for the Office of Privacy and Disclosure.

C. **Office of the Deputy Commissioner, Retirement and Disability Policy**
The Office of the Deputy Commissioner, Retirement and Disability Policy, is responsible for publishing in the Federal Register information that will guide the public as to how, where and when decisions are made. This includes statements of SSA's organization, functions and procedures, delegations of authority, and substantive rules of general applicability. This office also publishes Social Security Rulings, which index final decisions and opinions of a precedential nature.

D. **Regional and Central Office Freedom of Information Coordinators**
Each Associate Commissioner, Regional Commissioner and Program Service Center (PSC) Director has designated a FOI Coordinator to serve as the focal point for FOIA activities under his/her jurisdiction. Additional coordinators may also be designated. The responsibilities of the regional, PSC, and central office coordinators are to:

1. Provide technical guidance to regional/component staff on FOIA matters and to serve as liaison with the FOI Officer on disclosure policy matters.

2. Coordinate the handling of FOIA requests within the region or component, search for requested documents and provide them to OPD, and identify concerns about disclosure.

3. Maintain or collect regional/component data for SSA's Annual Report to the Attorney General on FOIA activity.

4. Coordinate the development and implementation of regional/component procedures for maintaining records of FOIA requests in compliance with the NARA records retention schedule and for capturing data needed for the annual report to the Attorney General on FOIA activities.

5. Coordinate regional/component training activities on FOIA matters.

6. Serve as the regional/component focal point for identification of materials required to be indexed under subsection (a)(2) of the FOIA and coordinate with OPD for indexing. See AIMS, GAM 14.12 for more information about indexing requirements.

14.13.05 Requests for Public Information Materials

A. **Public Information Materials**
We will not ordinarily consider requests for records that are normally prepared for public distribution, such as press releases, fact sheets, information brochures, or speeches, as FOIA requests. Provide such records promptly to any requester, without reference to the FOIA, without referral to OPD, and without any fee.

B. **Materials Published and Offered for Sale**
We will not consider requests for regulations or other material published in the Federal Register or material offered for sale through the U. S. Government Printing Office or the National Technical Information Service as FOIA requests. You may make these materials available for public inspection or refer the requester to the source for purchase of a copy or to a library which would maintain such materials.

C. **Requests for Information Only**
Do not consider requests for information only, such as explanations or answers to questions, as FOIA requests. Answer such inquiries promptly, as appropriate, without referral to OPD, as part of SSA's general effort to be responsive to the public.

14.13.06 Disclosures

A. **Disclosures Provided for by Regulations**
The following disclosures are provided for by regulation and do not require a determination by the FOI Officer. Any employee who is authorized within his or her organizational component to do so may make these disclosures. Additional guidance on disclosures is contained in AIMS, GAM 14.12. Component FOIA coordinators with

questions about whether or not a disclosure is appropriate should contact the Office of Privacy and Disclosure. OPD personnel can be located through the OGC Intranet page at http://ssahost.ba.ssa.gov/ogc/addresses phonelistings.cfm .

1. All disclosures authorized by SSA Regulations at 20 CFR Parts 401 and 402 .
2. All disclosures required by Federal law (other than the FOIA).
3. All disclosures from Privacy Act systems of records for which consent of the subject individual has been given or for which routine uses have been published.
4. All disclosures authorized by regulations of other Federal agencies from records subject to those regulations.

   Example: Disclosures of Federal employee information authorized by Office of Personnel Management (OPM) regulations at 5 CFR 293.311 .

   Example: Disclosures of procurement related information authorized by the Federal Acquisition Regulation (FAR) at 48 CFR Chapter 1 .
5. All material described in the Indexes of Administrative Staff Manuals and Instructions, unless otherwise noted.
6. All disclosures required by contracts or other legally binding agreements.

B. **Disclosures to the Federal Government and SSA Initiated Disclosures**
Disclosures to any part of the Federal government, State or local courts or legislatures, as well as SSA initiated disclosures, are not subject to the FOIA. Follow applicable regulations and instructions. If there are none covering the specific situation, the Commissioner, Deputy Commissioner, or Associate Commissioner responsible for the records, or the SSA Privacy Officer, the Systems Manager, or other official to whom authority has been delegated, will make the determination.

C. **Disclosure Determinations Not Covered Above**
Only the SSA FOI Officer may determine whether to release or withhold SSA records from the public in response to a FOIA request in situations not covered by sections AIMS, GAM 14.13.05 through AIMS, GAM 14.13.06B above.

14.13.07 Misdirected or Inadequate Requests

A. **Insufficient Identifying Information**
If a request clearly does not provide enough information to locate the requested records, return the request to the sender, explaining, if possible, the information we need to search for the records. Do not forward such requests to the FOI Officer.

B. **Records SSA Does Not Have**
If a request seeks records that SSA clearly does not have (e.g., the Social Security number of an individual who died in 1935), explain to the requester that we do not have the

requested records. If you do not know whether SSA would have the records, forward the request to the FOI Officer.

C. **Misdirected Requests**

1. **Requests That Do Not Require Action by the FOI Officer**

   If a request seems to provide enough information to locate the records, determine whether the requester is clearly entitled to the information under sections AIMS, GAM 14.13.05 through AIMS, GAM 14.13.06.B. above. If this is the case, but your office does not have the record, forward the request to the office that has the record. (If the record is easily obtainable, you may choose to obtain the record and reply to the requester.)

2. **Requests Requiring Action by the FOI Officer**

   If a request seems to include enough information to locate the records, but requires action by the FOI Officer, as in section AIMS, GAM 14.13.06.C. above, send the request directly to the SSA FOI Officer. Whether the material will be disclosed or withheld is not the determining factor. The FOI Officer will control the request and obtain the requested records.

14.13.08 Requests That Require Action by the SSA FOI Officer

A. **General**
All requests not covered by sections AIMS, GAM 14.13.05 through AIMS, GAM 14.13.06.B. above require action by the SSA FOI Officer. It does not matter whether the request will be granted or denied. Send requests to the SSA FOI Officer for response through the appropriate FOI coordinator. Hand carry or send via express mail or fax, as appropriate.

B. **Access Requests for Program Integrity Case Files or Other Privacy Act Exempt Systems of Records**
The Privacy Act Notice for a Privacy Act system of records maintained by SSA will state whether the system was published as exempt from the access provisions of the Privacy Act. SSA's Privacy Act Notices of Systems of Records are listed in SSA Pub. No. 65-009 . This publication is available on Social Security Online at https://www.ssa.gov/foia/bluebook/bluebook.htm . Consider a request for access by the person who is the subject of a file in one of these exempt systems of records as a FOIA request only if the systems manager decides that access should not be provided under the Privacy Act. Route such requests to the system manager identified in the system notice with a copy of the requested material. If the system manager decides that access will not be granted, he or she will forward the request with the material to the FOI Officer.

C. **Requests for DDS Records**
Requests for State Disability Determination Services (DDS) records may or may not be subject to the Federal FOIA. If a request involves records for which SSA has published a

Privacy Act Notice, we consider those to be SSA records. Other DDS records, such as personnel records, are not SSA records, and the DDS should process such requests according to State law. If a requester writes to SSA for such DDS records, advise the requester that these are not SSA records subject to the Federal FOIA and that he or she may wish to request the records from the DDS.

D. **All Other Requests**

1. SSA field offices or installations, including State Disability Determination Services, will send these requests to the regional FOI Coordinator for review. If appropriate, the regional FOI Coordinator will forward the request to the SSA FOI Officer.

2. All central office components will forward these requests to the component's FOI Coordinator. If the request involves records of more than one component, OPD will coordinate the response and prepare the final reply. Component FOI Coordinators should discuss any questions with OPD before forwarding the requests.

E. **Time Limits**

When forwarding a request to the FOI Officer, advise the requester that the statutory time limits do not begin until the FOI Officer receives the request.

14.13.09 Court Orders and Subpoenas for Production of Documents and Requests for Testimony

A. **Court Orders**

Bring all court orders for production of documents to the attention of the Regional Chief Counsel in the field or the Office of the General Counsel in central office.

B. **Regulations on Testimony**

SSA regulations at 20 C.F.R. Part 403 deal with requests for testimony by SSA employees and the production of records and information in legal proceedings to which SSA is not a party.

These rules do not apply when the request involves any of the following:

1. An SSA administrative proceeding;

2. A legal proceeding to which SSA is a party (“SSA” here includes the Commissioner and any employee acting in his or her official capacity);

3. A request from the U.S. Department of Justice;

4. A criminal proceeding to which the U.S. is a party;

5. A legal proceeding initiated by State or local authorities arising from an investigation or audit initiated by, or conducted in cooperation with SSA's Office of the Inspector General;

6. A request from either house of Congress (see AIMS, GAM 14.12);

7. A law enforcement proceeding related to threats or acts against SSA, its employees, or its operations ("SSA" here includes the Commissioner and any employee acting in his or her official capacity); or

8. A Federal law or regulation that expressly requires a Federal employee to provide testimony.

C. **Requests for Testimony**

1. Testimony is an oral or written statement to be given under oath or under penalty of perjury about any SSA function or any information or record created or acquired by SSA in the performance of its official duties. It may include the following:

   a. Any statement provided under oath or under penalty of perjury through personal appearance;

   b. Any statement provided under oath or under penalty of perjury through deposition;

   c. Any statement provided under oath or under penalty of perjury through recorded interview;

   d. Any statement provided under oath or under penalty of perjury by telephone, television or videotape;

   e. Any response (written or oral) provided under oath or under penalty of perjury during discovery or similar proceedings that would involve more than mere delivery of copies of records; and

   f. Any declaration made under penalty of perjury or any affidavit.

2. An SSA employee may not give testimony in a legal proceeding covered by these regulations unless the Commissioner or designee approves. Bring all requests for testimony to the attention of the Regional Chief Counsel in the field or the Office of the General Counsel in central office.

D. **Subpoenas Duces Tecum**

A subpoena duces tecum is a request for testimony and documents. SSA will no longer process subpoenas duces tecum as FOIA requests. Handle as in C. above.

14.13.10 Time Limits

The FOIA requires agencies to make a decision on whether to disclose information within 20 working days of receipt by the appropriate official. Agencies must decide appeals within 20 working days AIMS, GAM 14.12, The Freedom of Information Act, explains more about these time limits and when they may be extended.

14.13.11 Records Retention

See SSA's Operational and Administrative Records Schedules (OARS), accessible through the SSA Digital Library, for records retention requirements for FOIA requests and requested materials. Agencies must maintain FOIA requests and records requested from any office, whether disclosed or not, in accordance with the schedules, unless another records retention schedule requires maintaining them for a longer period of time. OPD will maintain records of requests and responses sent by OPD as well as FOIA appeals.

14.13.12 FOI Officer and FOI Coordinators

A. **SSA FOI Officer and OPD Staff**
The address and phone numbers for the SSA FOI Officer and OPD staff are available on the OGC intranet site at [redacted].

B. **Regional FOI Coordinators**
Addresses for the Regional FOI Coordinators are available on the OPD intranet site at [redacted].

C. **Component FOI Coordinators**
Addresses for Headquarters component coordinators are available on the OPD intranet site at [redacted].

A complete listing of SSA FOI Coordinators is available in the OPD public folder in Outlook. Inform OPD staff of any changes involving your component coordinator.

14.13.13 Authority

This Instruction is issued in accordance with applicable provisions of 5 U.S.C. 552 and SSA regulations: Privacy and Disclosure of Official Records and Information (20 C.F.R. 401) Availability of Information and Records to the Public (20 C.F.R. 402), Testimony by Employees and the Production of Records in Legal Proceedings (20 C.F.R. 403).

Freedom of Information Act Annual Report

Manual/Chapter: General Administration » Disclosure/Confidentiality of Information
Instruction/Handbook: GAM 14.15
Audience: General
Level: SSA
Inquiries: Office of Privacy and Disclosure (OPD) | [redacted]@ssa.gov | 410-966-6645
Related Instructions: Office Of The General Counsel (OGC) » Office of Privacy and Disclosure (OPD)
Updated: 7/17/2020
Certified: *(not yet certified)*

Table of Contents

14.15.01 Purpose

This instruction describes the reporting requirements of the Annual Report and the information to be collected in completion of the Social Security Administration's (SSA) report.

At the close of the fiscal year (FY), i.e. September 30th, each Federal agency must provide an annual report of their Freedom of Information Act (FOIA)/Privacy Act (PA) activities to the Department of Justice (DOJ) by February 1st of the following year.

14.15.02 General

A. The Office of Privacy and Disclosure (OPD) is responsible for notifying the regional and central office FOIA Coordinators of how and when to complete the FOIA report. The

report and instructions for completion are provided online at: [redacted] . To make reporting easier, the regions should complete the report at least once a month.

B. Central office coordinators should complete the report when responding to a FOIA/PA request and provide staff hours used to search for information for OPD.
NOTE: Components may have staff hours even if no requests are received.

C. At the end of the FY, OPD collects this data and prepares the final report. (See Attachment Guidelines for Agency Preparation of Annual FOIA Reports and Attachment Submitting the Annual Report)

14.15.03 Definition of a Request/Information to be Reported

A. Definition of a Request
A FOIA/PA request is a request for existing records in the possession of SSA from a member of the public. Any office may receive a request for records under the FOIA/PA. The request need not cite the FOIA/PA. It is a good policy to treat all first-party access requests as FOIA/PA requests regardless of whether the FOIA/PA is cited.

B. Information to be Reported

1. The following are examples of some general types of FOIA/PA requests:

- Requests for manuals (POMS, AIMS, etc.), memorandums, reports or management information records;
- Access requests from individuals or their authorized representative, a parent or legal guardian of a minor child. (Note: if the request is sent to OPD for denial do not count it on the report, OPD will count it);
- Requests from individuals for information pertaining to others with consent; (Examples of items to include: benefit verifications, SSN verifications, benefit statements, folder requests and other requests for personal information)
- Requests for contract documents.

2. The following are examples of requests NOT reported as FOIA/PA requests:

- Requests for publications and other information materials produced specifically for public distribution. (AIMS,GAM 14.13.05, Request for Public Information Materials, explains such requests in more detail.);
- Requests for materials that are published in the Federal Register or offered for sale through the U. S. Government Printing Office;
- Requests for information that can be disclosed under an applicable routine use, provided a statement of routine use associated with a particular system of records has been published in the Federal Register. (See POMS GN 03313 , 03314 or a PA System of Records);

- Requests for explanations of policies or procedures, the status of claims, and general information about SSA programs (AIMS,GAM 14.13.05c.1);
- Requests from Federal agencies and Federal and state courts.

14.15.04 Completion of the Final Report

OPD is responsible for completion of the final report and submittal to DOJ. The information needed to complete the report accurately is:

A. The number of FOIA/PA requests responded to,

B. The total fees collected,

C. Staff cost, which would include copying records and mailing costs,

D. Training on FOIA, i.e., instructor and trainee, and

E. The cost of preparing the report.
NOTE: Staff cost is the hourly rate of the employee. (See Attachment Annual Report Guidance Outline & Template)

14.15.05 Attachments

Attachments: Guidelines for Agency Preparation of Annual FOIA Reports
Submitting the Annual Report
Annual Report Guidance Outline & Template

Access to, and Monitoring of, Employee-Generated Electronically Stored Information (ESI) on Agency Information Technology Systems, Network Devices, or Government Office Equipment

Manual/Chapter: General Administration » Disclosure/Confidentiality of Information
Instruction/Handbook: GAM 14.16
Audience: General
Level: SSA
Inquiries: Office of General Law (OGL) | [redacted]@ssa.gov , [redacted]@ssa.gov
Related Instructions: Office Of The General Counsel (OGC) » Office of General Law (OGL)
Updated: 11/7/2023
Certified: 1/13/2021

Table of Contents

14.16.01 Purpose

This instruction provides guidance to agency management official(s) seeking access to, or monitoring of, employee-generated ESI on agency information technology (IT) systems, network devices, or Government office equipment.

14.16.02 Objective

The objective of this instruction is to ensure that access to, and monitoring of, employee-generated ESI on agency IT systems, network devices, or Government office equipment complies with applicable laws and regulations.

14.16.03 Definitions

For the purpose of this policy, the following definitions apply:

A. **Electronically Stored Information (ESI):** ESI refers to any electronic or digital information, including documents and files; email and email storage files; phone records; texts and voicemail messages; audits, or Internet usage, located on, or maintained by, the agency's IT systems, network devices, or Government office equipment, including servers, computer units, phones, facsimiles, laptops, or portable electronic devices

B. **Employee:** Employee refers to any individuals who have access to Social Security Administration (SSA) systems, including SSA employees, contractors, State Disability Determination Services employees, and volunteers.

C. **Protected Disclosure:** A protected disclosure may include the disclosure of information that the employee reasonably believes evidences: (a) a violation of any law, rule, or regulation, or (b) gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety.

D. **Agency Record:** Agency records are all books, papers, maps, photographs, machine-readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the U.S. Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value of data in them. This definition includes certain types of electronic messages or documents.

14.16.04 Scope

A. This policy applies to:
Requests made by agency management official(s) to access or to monitor employee-generated ESI, including, but not limited to, access to investigate possible misconduct.

B. This policy does not apply to:

1. Access to, or monitoring of, employee generated ESI for the sole purpose of obtaining agency record(s) when the employee is absent from work and there is a work related exigency. If a manager needs access to an absent employee's ESI for a work-related exigency, after exhausting other reasonable avenues to obtain the agency record(s), management must inform the absent employee of the access or monitoring within a reasonable amount of time after the employee's return to work.

2. Access to, or monitoring of, employee generated ESI in connection with any statutory or legal requirements, or in connection with any routine system security or integrity review (e.g., Audit Trail System, Control Audit Test Facility, or Onsite Security Control Audit Reviews), audit, administration, or maintenance, including monitoring related to national security or the Federal Information Security Management Act of 2002.

3. Requests under the Freedom of Information Act or Privacy Act;

4. Requests from law enforcement;

5. Requests from the Office of Special Counsel;

6. Requests from either House of Congress;

7. Requests from the Office of the Inspector General or Government Accountability Office concerning audits or investigations; or

8. Requests from the Office of the General Counsel (OGC) related to the preservation or production of ESI in legal matters.

14.16.05 Policy

Employees do not have a right, nor should they have any expectation of privacy while using any agency computer system, enterprise network, or Government office equipment at any time. By using such agency property, employees consent to monitoring, intercepting, recording, using, or disclosing the contents of ESI.

Only the delegated agency official(s) may authorize access to, or monitoring of, employee-generated ESI. Agency management officials seeking to access or to monitor employee generated ESI must submit a written request identifying the nature and scope of the requested ESI and supporting justification. The nature and scope of the requested ESI to be accessed or monitored must be appropriately tailored to the justification.

No one may access or seek to access ESI to target protected disclosures or for other improper purposes, including reprisal or discrimination.

14.16.06 Procedure

A. Before initiating a request to access or to monitor employee generated ESI, agency management official(s) must consult with an OGC attorney to ensure that the requested access is justified at its inception and permissible in scope. Operations employees should follow existing protocols for contacting OGC. Headquarters and regional OGC contacts can be found at Office of the General Counsel | Our Organization [redacted] .

B. After consulting with an OGC attorney, agency management official(s) must initiate a written request, including the nature and scope of the requested ESI and supporting justification. The requestor must send the written request through the appropriate management channel(s) to the component's designated individual(s) for entry into the Access to ESI Data Request System maintained by the Office of Chief Information Officer. Only those with approved rights should complete the form, which can be found at Service Catalog SSA | Service Portal [redacted] . Supporting justifications must provide the reason(s) for the requested access or monitoring. For example, if the reason concerns suspected misconduct, the request must include a statement about the suspected misconduct and how the requested ESI relates to the suspected misconduct.

C. The Access to ESI Data Request System will notify the component Deputy Commissioner level official for review and approval. Once approved at the component Deputy Commissioner level, the Access to ESI Data Request System will direct copies of the request to delegated agency level official(s) for review and approval. The approving official may return any vague or overbroad request for additional clarification or further information. Improper requests will be denied.

D. ESI and records documenting the initiation, review, and approval of access to, or monitoring of, employee generated ESI, including the opinions and recommendations of OGC, must be retained in accordance with the applicable agency or Government-wide record schedules, or longer, if subject to a Litigation Preservation or Hold.

1. The applicable record schedule may differ depending on the reason for the request for access or monitoring, or type of ESI.

2. Information regarding record schedules may be found in the below references. You may direct questions regarding retention periods to SSA's Records Management Staff.

3. Recipients of the data are responsible for protecting, handling, and disclosing ESI in accordance with policy, regulation, and law.

4. The applicable policy, regulation, and law may differ depending on the reason for the request for access or monitoring or type of ESI.

5. Information regarding protecting, handling, and disclosing ESI may be found in the below references. You may direct questions regarding protecting, handling, and disclosing any personally identifiable information found in the ESI to the Office of Privacy and Disclosure.

14.16.07 General Provisions

A. SSA will enforce this policy consistent with applicable law. Failure to comply with this policy may result in appropriate corrective action, including disciplinary action or criminal prosecution.

B. Nothing in this policy creates any enforceable rights.

14.16.08 Delegations of Authority

You will find the Delegations of Authority for approving requests for access to ESI generated by employee activity or use under this policy at [redacted]

14.16.09 References

You will find information regarding the use of any agency computer system, enterprise network, or Government office equipment in the Annual Personnel Reminders and Information Security Policy .

For information regarding protections and rights under the Whistleblower Protection Act and Whistleblower Protection Enhancement Act, please visit the Office of the Inspector General or the U.S. Office of Special Counsel websites. For information regarding agency Equal Employment Opportunity policies, please visit the Office of Civil Rights and Equal Opportunity website.

For information regarding SSA specific and General Records Schedules, please visit [redacted] .

For information regarding protecting, handling, and disclosing ESI in accordance with policy, regulation and law, please reference GAM 15.01 - 15.08, available at General Administration Manual (GAM).

Agency Litigation Preservation Policy

Manual/Chapter: General Administration » Disclosure/Confidentiality of Information
Instruction/Handbook: GAM 14.17
Audience: General
Level: SSA
Inquiries: Office of General Law (OGL) | [redacted]@ssa.gov , [redacted]@ssa.gov
Related Instructions: Office Of The General Counsel (OGC) » Office of General Law (OGL)
Updated: 1/13/2021
Certified: 1/13/2021

Table of Contents

14.17.01 Purpose

This instruction provides guidance and internal procedures to agency employees regarding the agency's Litigation Preservation Policy (Policy). Whenever civil litigation is pending or reasonably anticipated, including some threats of litigation, the agency must take reasonable and good faith action to preserve potentially relevant information, documents, and other tangible things. Agency attorneys have a responsibility to work with the agency witnesses and custodians of records to ensure that these individuals understand and comply with the agency's preservation obligations, take the necessary steps to identify and preserve material, and maintain it in proper formats.

This instruction further describes the scope of, and the legal authority for, the Policy. In addition, this instruction explains the circumstances that can give rise to the agency's obligation to preserve information, documents, or other tangible things. This Policy provides details regarding issuing a Litigation Hold, the information, documents, and tangible things subject to a Litigation Hold, and the obligations of the custodians of records pursuant to a Litigation Hold. This Policy also provides guidance regarding preserving the information, data, documents, records, and tangible things when litigation may be foreseeable, as well as during the course of the litigation. Finally, this Policy describes the process by which a Litigation Hold will be released. Adhering to this Policy should ensure that the agency fulfils its legal obligations and preserves the material needed to defend or pursue its legal rights.

14.17.02 Objective

The objective of this instruction is to ensure that the agency fulfills its preservation obligations in compliance with applicable laws and regulations.

14.17.03 Definitions

For the purpose of this Policy, the following definitions apply:

A. **Potentially Relevant Information may include:**

i. **Electronically stored information (ESI), including, but not limited to:** any electronic or digital information, including word processing documents, files, spreadsheets, and calendars; email and email storage files; phone records; texts and voicemail messages; audits, computer modeling runs, databases, applications (e.g., Microsoft Outlook, Word), videos, sound recordings, Internet usage, and micrographic (e.g., microfilm and microfiche); cartographics (e.g., maps, architectural and engineering drawings); network server information; or claims file records.

ii. **Paper records and documents or paper stored information (PSI), including but not limited to:** files; folders; calendars; notes; correspondence; drafts; policies; manuals; leave slips; worksheets; memoranda; reports; information or documents printed to hard or paper copies; or handwritten information or documents.

iii. **Equipment, including but not limited to:** agency computers and laptops; portable or removable storage media (e.g., CDs, DVDs, external drives); servers, including data servers containing file shares and Microsoft Exchange servers containing emails; or cell phones and personal digital assistants (e.g., BlackBerrys). Equipment may include an employee's personal device, if there is reasonable expectation that the employee's personal device contains information that is potentially relevant to pending or anticipated litigation involving the agency.

B. **Documents:** all electronic and non electronic documents and data as well as tangible materials, including agency records and non-record materials made, sent, received, or

stored in the transaction of SSA business or on SSA equipment, as well as personal records that are relevant to litigation involving the agency. See 44 U.S.C. § 3301 and 36 C.F.R. § 1220.18.

C. **Employee (or Custodian):** any individuals who have access to information, documents, or other tangible things on SSA systems, including SSA employees, contractors, State Disability Determination Services (DDS) employees, and volunteers.

D. **Litigation Hold:** an instruction to preserve documents potentially relevant to any party's claim or defense or in pending or anticipated litigation.

14.17.04 Scope

This Policy covers the internal procedures that all SSA Employees must follow when they have access to, or control over, potentially relevant information related to pending or reasonably anticipated litigation in a civil, criminal, or administrative proceeding. If a Litigation Hold is issued, applicable document destruction schedules are suspended and documents subject to the Hold must not be destroyed. Employees must preserve information, documents, and other tangible things in the native format including metadata.

14.17.05 Policy

Whenever the agency is involved in civil litigation or "reasonably anticipates litigation, it must suspend its routine document retention and destruction policy and put in place a 'litigation hold' to ensure the preservation of relevant documents." *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212, 218 (S.D.N.Y. 2003); see also *Victor Stanley, Inc. v. Creative Pipe, Inc.*, 269 F.R.D. 497, 521 (D. Md. 2010) (duty to preserve is imposed by common law). A reasonable anticipation of litigation arises when the agency is on notice of a credible probability that it will become involved in litigation, seriously contemplates initiating litigation, or takes specific actions to commence litigation. The duty to preserve arises whether the legal action is brought by or against the agency, (i.e., it does not matter if the agency is the Plaintiff or Defendant in the matter; if the agency reasonably anticipates litigation, a litigation hold should be instituted).

Litigation preservation is the agency's responsibility. As legal counsel for the agency, OGC is responsible for issuing and overseeing Litigation Holds in order to enable the agency to fulfill its duty to preserve. Determining whether the agency can reasonably anticipate litigation is a fact based inquiry requiring OGC to evaluate the relevant facts and circumstances and assess whether those facts and circumstances trigger the agency's litigation preservation obligations. Later information may require reevaluation of whether a Litigation Hold is necessary. If the initial circumstance makes the necessity of a Litigation Hold unclear, a Litigation Hold should be issued, and then quickly terminated when OGC has determined that the matter has concluded and no further legal action or appeals are anticipated or known. If an agency employee or manager suspects that a particular event or series of events creates a reasonable anticipation of litigation for the agency, the employee or manager should consult OGC, as appropriate.

14.17.06 Procedure

A. Whenever the agency is involved in civil litigation or "reasonably anticipates litigation," the employee must preserve all information that may be relevant to the litigation. Upon receiving a Litigation Hold notice, the employee should preserve in-place all potentially relevant information and must suspend any routine document retention and destruction policies or practices. On a case-specific basis, the employee should follow the specific guidance set forth in the Litigation Hold notice and contact the OGC attorney named in the Litigation Hold notice with any questions about the Hold.

B. **Issuing the Litigation Hold:**

i. **OGC identifies Custodians and the Information to be Preserved:** once OGC determines that the agency has a duty to preserve, OGC will identify possible custodians of information, documents, or other tangible things subject to the Litigation Hold and contact the custodians to assist in identifying, locating, and preserving relevant information. Custodians may include information technology (IT) employees, record keeping managers, or data owners of potentially relevant information such as contractors, supervisors, managers, or other employees associated with the pending or reasonably foreseeable litigation.

ii. **Issuing the Litigation Hold:** when appropriate and within a reasonable period after notice of pending litigation or after litigation becomes reasonably foreseeable, OGC (or the Department of Justice (DOJ) in some cases where DOJ has litigation responsibility for the matter) will issue a Litigation Hold to each identified custodian or potential custodian. OGC will ask Custodians to verify receipt and compliance with the instructions in the Litigation Hold. See number vii below.

iii. **Cases Involving Records Transferred to a Record Center:** if the agency needs to preserve records that the agency already transferred to a record center, OGC will work with the Center for Records Management to ensure the records are preserved.

iv. **When an Employee Has Changed Jobs or Left SSA:** the agency's obligation to preserve relevant electronic or other documents remains after an employee leaves the agency or changes jobs until the Litigation Hold is lifted. The agency policy covering Removal of Records and Paper Upon Separation or Transfer from SSA is found at AIMS, Chapter 7 of the Material Resources Manual Removal of Records and Papers Upon Separation or Transfer from SSA Chapter.

v. **Maintaining the Litigation Hold:** until the agency releases the Litigation Hold, Custodians must preserve information, documents, or other tangible things subject to the Litigation Hold. OGC will periodically remind Custodians that the hold is in effect and that they have an ongoing obligation to preserve information, documents, or other tangible things subject to the Litigation Hold.

vi. **Bargaining Unit Employees:** OGC may issue a Litigation Hold to a bargaining unit employee who is a custodian of relevant information.

vii. **Confirming Understanding of Obligation to Preserve:** in accordance with the Litigation Hold, Custodians must acknowledge in writing or electronically to OGC that they have read and understand their continuing obligations under the Litigation Hold.

C. **Releasing the Litigation Hold**

Custodians must continue to preserve information, documents, or other tangible things subject to the Litigation Hold until OGC or DOJ notifies them that the hold has been released. Custodians must not release or lift the Litigation Hold until so directed in writing by OGC or DOJ.

14.17.07 General Provisions

A. SSA will enforce this policy consistent with applicable law. Failure to comply with this policy may result in appropriate action, including disciplinary action.

B. Nothing in this policy creates any enforceable rights.

14.17.08 References

You may find the following authorities helpful in more fully explaining the agency's litigation preservation obligations:

- Fed. R. Civ. P .26(b)(1) ("[p]arties may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense and proportional to the needs of the case. . . . Information within this scope of discovery need not be admissible in evidence to be discoverable.")
- Fed. R. Civ. P. 37(b), (e) (Once a party's duty to preserve arises, a failure to preserve relevant information could result in sanctions.)
- Fed. R. Civ. P. 37(f) Advisory Committee's Notes ("When a party is under a duty to preserve information because of pending or reasonably anticipated litigation, intervention in the routine operation of an information system is one aspect of what is often called a 'litigation hold'.")
- Fed. R. Civ. P. 16, 26, 33, 34, 45 (Other Discovery/Preservation-Related Rules)
- 44 U.S.C. § 2909 (general retention of records by federal agencies and delegation to Archivist of the National Archives and Records Administration for retention schedules)
- *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212, 218 (S.D.N.Y. 2003); see also *Victor Stanley, Inc. v. Creative Pipe, Inc.*, 269 F.R.D. 497, 521 (D. Md. 2010) (duty to preserve is imposed by common law)

- *Silvestri v. Gen. Motors Corp.*, 271 F.3d 583, 591 (4th Cir. 2001) ("The duty to preserve material evidence arises not only during litigation but also extends to that period before the litigation when a party reasonably should know that the evidence may be relevant to anticipated litigation.")

Component Roles and Responsibilities Regarding PII

Manual/Chapter: General Administration » Personally Identifiable Information (PII) Loss and Remediation
Instruction/Handbook: GAM 15.01
Audience: General
Level: SSA
Inquiries: Office of Privacy and Disclosure (OPD) | [redacted]@ssa.gov | 410 966 6645
Related Instructions: Office Of The General Counsel (OGC) » Office of Privacy and Disclosure (OPD)
Updated: 7/17/2020
Certified: *(not yet certified)*

Table of Contents

15.01.01 Purpose of Instruction

The information in the chapters of this series of AIMS materials provides agency policy defining the roles and responsibilities of agency employees, components and contractors regarding protection of PII, PII breaches and associated tasks required by the Office of Management and Budget (OMB). This AIMS guide codifies and supersedes prior agency guidance.

15.01.02 Authorities and References

A. *Privacy Act of 1974* as amended (5 U.S.C. 552a) (Privacy Act of 1974)

B. OMB Memo M 06 15, Safeguarding Personally Identifiable Information, May 22, 2006

C. OMB Memo M 06 19, Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments, July 12, 2006

D. Recommendations for Identity Theft Related Data Breach Notification, September 20, 2006

E. OMB Memo M-06-16, Protection of Sensitive Agency Information, June 23, 2006

F. OMB Memo M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, May 22, 2007

G. Federal Information Processing Standards Publication 199: Standards for Security Categorization of Federal Information and Information Systems

H. The Federal Information Security Management Act (FISMA) of 2002, 44 U.S.C. § 3541

I. Information Security Policy (ISP)

J. National Institute of Standards and Technology (NIST) Special Publication 800 122 Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)

K. M-15-01, Fiscal Year 2014-2015 Guidance on Improving Federal Information Security and Privacy Management Practices

15.01.03 Overall Responsibility for Protection of Information at SSA

One of the main Federal statutes mandating protection of personal information is the Privacy Act of 1974 as amended (5 U.S.C. 552a). Anyone working for or on behalf of the Social Security Administration (SSA) is responsible for protecting information that has been entrusted to the agency[1]. Some agency staff have been given specialized security training (e.g., component or local secure officers (CSOs or LSOs) and are important local resources that can assist employees and management in fulfilling this duty. An important part of this duty is to ensure that PII is properly collected, used, protected, and discarded.

15.01.04 Shared Component Responsibilities for Policy that Protects PII

While everyone at SSA has a duty to protect the information in the agency's care, historically, the responsibility for writing the policies and defining the procedures and processes used in doing that task have been shared across the agency.

For example, discussions about PII could touch upon or require familiarity with issues and existing agency policies and procedures in areas pertaining to privacy, information technology (IT) security, physical security, the Freedom of Information Act, the Privacy Act , records retention and records management. Administrative policies such as resource management and property disposal and human resource issues such as Telework, labor agreements and the roles and duties of employees and managers under applicable federal law and regulation could also be PII-related or have an impact on protecting PII.

The responsibility for agency policy and procedures for these areas resides in a number of components, and although many of these were not written specifically to protect PII, the fact is that they often do provide important guidance that is to be followed. It is important then to ensure all agency stakeholders work together and coordinate their policies and procedures as they relate or impact PII, and unless it is clearly stated otherwise, the policies in this Chapter are not intended to replace or override other agency policies but instead to complement and work along with them.

The following list is not all inclusive and will be updated as components change. Refer to Appendix B of Information Security Policy (ISP) for more specific listings of roles and responsibilities.

A. **Systems**

1. Under FISMA , the agency's Chief Information Officer (CIO) is responsible for IT security. At SSA, the Office of Chief Information Officer (OCIO) is also the agency's CIO. At the direction of the Commissioner of Social Security, the CIO has been named the lead for addressing OMB PII directives.

2. The agency Chief Information Security Officer (CISO) is the agency PII Incident Coordinator and chairs the PII Incident Response Group (See AIMS GAM 15.05)

3. In addition, Systems performs IT operational tasks and implements technical systems and IT solutions across the agency that conform to the government-wide and agency IT security policies. Because much of the data used by the agency is PII, Systems plays a major role in the protection of PII.

4. OS works closely with the Office of General Counsel (OGC), and Office of Budget, Financ, Quality, and Management (OBFQM) since privacy, PII and security policies and procedures are all interrelated.

B. **The Office of General Counsel (OGC)**

1. The privacy of data is closely linked to, but separate from, the security of data. OMB Memo M 05 08 required each agency to appoint a Senior Agency Official for Privacy (SAOP). This senior official has overall responsibility and accountability for ensuring the agency's implementation of information privacy protections. At

SSA, the General Counsel is the appointed SAOP. The SAOP has a central role in overseeing, coordinating and facilitating the agencies compliance efforts, including the Privacy Act. (See AIMS, GAM Chapter 14 for more information.)

2. Because privacy and security are very closely related, OGC works closely with OS. Likewise, OGC also works very closely with OBFQM and Systems, since privacy, PII and security policies and procedures are all interrelated. In addition, OGC is responsible for Privacy Impact Assessments (PIAs).

C. **Office of Budget, Finance, Quality, and Management (OBFQM)**

1. OBFQM has various responsibilities that impact PII. These include physical security policy, security compliance policy, records retention and management policy, administrative policies, financial management and contracting policies. These activities often either involve PII or have an impact on protecting sensitive data, which often includes PII. (More specific information can be found in various areas of the AIMS guide.)

2. OBFQM works closely with OGC and Systems, since privacy, PII and security policies and procedures are all interrelated.

15.01.05 Component Responsibilities for Protection of Agency Information

- All agency components (including the Disability Determination Services (DDSs)) either "own" (see ISP 6.1) or use various agency administrative or programmatic resources that contain PII. They are responsible for ensuring **all** agency rules and policies, including those about PII, are applied or followed by their employees and contractors and grantees. Components are responsible for ensuring their employees are aware of agency level policies and providing them with component level policy and procedure regarding PII. Responsibility for ensuring components are aware, trained and comply with agency policy has been given to the agency's Deputy Commissioners (or equivalent) for their individual component.

A. In addition, in the event of a PII incident, the Deputy Commissioner or equivalent level official of a component that experiences a PII loss or is responsible for ensuring that the component responds to the PII breach in accordance with agency policy. (See also AIMS, GAM 15.02.)

B. Deputy level components are required to identify designated individuals (i.e., CSOs, LSOs, key management personnel) who will be routinely notified whenever a PII loss report originates from within their component. This process should ensure that component management at key levels is aware of PII loss incidents and has timely information about them. (See GAM 15.02.)

C. Components with responsibility for putting information online onto either the agency's Internet or Intranet web sites must ensure that activities comply with all

agency rules and requirements[2] including those involving disclosure and PII. Responsibility for protecting information (including PII) does not change simply because of the media involved (e.g. paper, electronic or online). All information made available online is still covered by long standing agency policies regarding privacy and disclosure and must comply with those rules. Questions on whether something is appropriate for posting online must be resolved prior to taking the action.

15.01.06 Applicability to Contractors

Contractors, including subcontractors and grantees doing business with SSA are required to adhere to all applicable rules, regulations, etc, including those related to PII protection and PII loss. Language has been prepared that adds appropriate PII policy into contracts and grants that require it. The Office of Acquisition and Grants works with Contracting Officers Technical representatives or Project Officers to ensure contracts or grants have the appropriate clauses, including those related to PII. (See also 15.02.)

15.01.07 Questions on PII Policy

Questions about PII should be directed to component management (i.e., a supervisor or manager) or your component security officer (CSO). Questions related to disclosure may be addressed to the Office of Privacy and Disclosure (OPD) in OGC.

15.01.08 Definitions

Breach SSA has adopted OMB's definition of breach (see OMB M 07 16). For the purposes of this policy, the term "breach" includes the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for other than authorized purposes have access or potential access to PII, whether physical or electronic.

Employee - Employee includes both agency and DDS employees.

Harm – Physical, psychological or economic injury or damage. Breaches may comprise a broad range of harm to individuals, including the potential for economic or medical identity theft. OMB requires agencies to consider a wide range of harm associated with the loss or compromise of information, such as harm to reputation and the potential for harassment or prejudice, particularly when health or financial benefits information is involved in the breach. Such harm may also include the effect of a breach of confidentiality on fiduciary responsibility, the potential for blackmail, the disclosure of private facts, mental pain and emotional distress, the disclosure of address information for victims of abuse, the potential for secondary uses of the information which could result in fear or uncertainty, or the unwarranted exposure leading to humiliation or loss of self-esteem.

Identity Theft – Identity theft and identity fraud are terms used to refer to all types of crimes in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain.

Incident – See Breach

Level of Impact – Impact levels low, moderate, and high describe the worst case potential impact on an organization or individual, if a breach of security occurs. Impact levels are defined by the National Institute of Standards and Technology (NIST) in FIPS 199 . As of the date of publication, those are defined as follows:

- **Low:** The loss of confidentiality, integrity, or availability is expected to have a limited adverse effect on organizational operations, organizational assets or individuals.
- **Moderate:** The loss of confidentiality, integrity, or availability is expected to have a serious adverse effect on organizational operations, organizational assets or individuals.
- **High:** The loss of confidentiality, integrity, or availability is expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets or individuals.

Linkable The National Institute of Standards and Technology has defined linkable in SP 800 122 . Linkable information is information about or related to an individual for which there is a possibility of logical association with other information about the individual. For example, if two databases contain different PII elements, then someone with access to both databases may be able to link the information from the two databases and identify individuals, as well as access additional information about or relating to the individuals. If the secondary information source is present on the same system or a closely related system and does not have security controls that effectively segregate the information sources, then the data is considered linked. If the secondary information source is maintained more remotely, such as in an unrelated system within the organization, available in public records, or otherwise readily obtainable (e.g., internet search engine), then the data is considered linkable.

Linked - The National Institute of Standards and Technology has defined linked in SP-800-122 . Linked information is information about or related to an individual that is logically associated with other information about the individual.

Logging – OMB M 06 16 requires agencies to keep a log when data is extracted from their agency repositories and to account for the disposition of the information. In this situation, a log file is a record containing basic identifying information about the data being moved that allows the agency to know that appropriate safeguards and controls are applied. (See AIMS, GAM 15.03.01.)

Managers - For purposes of this policy includes not just members of management but also designated employees who have been authorized to report PII losses (e.g., COTR POC).

NNSC National Network Service Center is the agency help desk that can be reached by phone at [redacted] The NNSC is available 24 hours per day, 7 days per week, 365 days per year.

Personally Identifiable Information (PII) – Effective May 2010, SSA uses the National Institute of Standards and Technology definition found in SP 800 122 : "PII is any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information."

Obsolete Prior to May 2010, SSA used OMB's definition of PII (see OMB M 07 16). The term "personally identifiable information" refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

Reportable PII Loss PII loss is defined as any information in paper or electronic format containing PII collected and maintained as part of SSA's business processes, which the Agency has reason to believe has left its custody, or has been disclosed to an unauthorized individual or entity, in circumstances that could lead to its misuse.

Risk – The possibility of harm or injury. With regard to a breach of PII, risk is defined as the likelihood of injury or harm caused to an individual whose PII is the subject of such breach.

SSA's secure environment is comprised of the high level systems (and their appropriate subsystems) described in our annual FISMA report.

Trusted systems - are external to SSA. Data transmission to a trusted partner is governed by a formal agreement that requires compliance to the same laws and/or regulations or equivalent standards as SSA (i.e., FISMA , Privacy Act , Federal Acquisition Rules, OMB directives, SSA security rules, compliance and auditing requirements). A Trusted system/partner organization may have a number of systems, not all of which are considered trusted systems unless they each have the appropriate formal agreements in place.

US-CERT – United States Computer Emergency Readiness Team of the Department of Homeland Security. SSA is required to report security and PII incidents to this organization.

[1] In 1937, the Social Security Board established Regulation No. 1 which establishes agency policy to protect the privacy of individuals to the fullest extent possible while nonetheless permitting the exchange of records required to fulfill our administrative and program responsibilities. In 1939, Congress enacted Section 1106 of the Social Security Act which became the statutory basis for maintaining the confidentiality of information collected by SSA. This section provides, in part, that no disclosure of any file, record, report, paper, or other information obtained at any time by the Commissioner of SSA or by any officer or employee of SSA in the course of discharging the duties of the Commissioner shall be made except as provided by SSA regulations or except as provided by Federal law. These statutory and regulatory provisions indicate the importance that Social Security's founders placed on protecting PII.

[2] SSA Web Governance Policies

Reporting the Loss of PII

Manual/Chapter: General Administration » Personally Identifiable Information (PII) Loss and Remediation
Instruction/Handbook: GAM 15.02
Audience: General
Level: SSA
Inquiries: Office of Privacy and Disclosure (OPD) | [redacted]@ssa.gov | 410 966 6645
Related Instructions: Office Of The General Counsel (OGC) » Office of Privacy and Disclosure (OPD)
Updated: 8/4/2020
Certified: *(not yet certified)*

Table of Contents

15.02.01 Purpose of Instruction

A. The information in this chapter provides the policy and procedures that agency (including DDS) employees and contractors must follow in the event of the loss or suspected loss of PII.

B. OMB M 15 01 requires agencies to report confirmed cyber PII incidents to US CERT and to report confirmed paper PII incidents to the agency privacy office, within one hour.

To avoid under or late PII incident reporting, SSA does not distinguish between potential and confirmed breaches. SSA's policy is to report all PII incidents confirmed or

suspected within one hour to PII Loss Reporting Tool.

The polices provided here regarding PII incident reporting and responsibilities do not replace but rather complement requirements for Federal agencies report security incidents in accordance with NIST Special Publication 800 61 .

15.02.02 Authorities and References

A. *Privacy Act of 1974* as amended (5 U.S.C. 552a) (Privacy Act of 1974)

B. OMB Memo M 06 15, Safeguarding Personally Identifiable Information, May 22, 2006

C. OMB Memo M 06 19, Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments, July 12, 2006

D. Recommendations for Identity Theft Related Data Breach Notification, September 20, 2006

E. OMB Memo M-06-16, Protection of Sensitive Agency Information, June 23, 2006

F. OMB Memo M 07 16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, May 22, 2006

G. Federal Information Processing Standards Publication 199: Standards for Security Categorization of Federal Information and Information Systems

H. The Federal Information Security Management Act (FISMA) of 2002, 44 U.S.C. § 3541

I. Information Security Policy (ISP)

J. National Institute of Standards and Technology (NIST) Special Publication 800 122 Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)

K. M-15-01, Fiscal Year 2014-2015 Guidance on Improving Federal Information Security and Privacy Management Practices

15.02.03 Handling PII Loss Reports from Contractors

A. The agency is responsible for reporting to the United States Computer Emergency Readiness Team (US-CERT) cyber losses of SSA PII by contractors (hereinafter to include subcontractors) and grantees working for SSA. The agency is responsible for reporting to the agency privacy office paper losses of SSA PII by contractors (hereinafter to include subcontractors) and grantees working for SSA.

B. Program officials charged with technical oversight for contracts and those for grants (contracting officer technical representative (COTRs) and project officers (POs) respectively) are expected to ensure their contractors and grantees understand what PII

is and what this responsibility means to them in the context of their engagement. They must ensure they understand their responsibilities and obligations to protect PII and to report any incident to the agency. (See AIMS, GAM 15.01)

C. Individuals named as agency contacts or liaisons will be the point of contact (POC) for contractor or grantee PII incident reports, and these POCs must take the PII incident reports from the contractor or grantee and report the incident to the National Network Service Center (NNSC). (For purposes of this policy, the POC should follow the guidance provided for managers in 15.02.03.B below.) In situations where it is not possible to timely contact the POC, contractors or grantees may file the report directly.

D. The agency decision maker works with the PO or the COTR to ensure the incident is remediated appropriately in accordance with agency security policy, protocol and procedure and to apply the breach notification plan (BNP) (AIMS, GAM 15.06) to determine if notice will be necessary.

15.02.04 Procedure for Reporting a PII Loss

A. In responding to or reporting an incident, do not further compromise the information involved in the PII incident (e.g., SSN, full name, birth date, etc.) by forwarding the PII to anyone without a need for that specific level of detail. Redact reports for those who do not need the specific PII.

B. If your supervisor/manager, component security officer (CSO) or the NNSC requires copies of the compromised PII or information about it in order to respond to the incident, they will give you instructions on how and to whom you should send the compromised information.

C. If a device or media was encrypted, the loss should still be reported as a (potential) PII incident. While the encryption protection likely means that we will determine there to be no exposure of the data, that determination remains a separate issue and does not relieve us of the responsibility to report the loss.

D. **Employee Procedures**

1. When employees, including disability determination service (DDS) employees, lose or suspect the loss of PII (paper or electronic), they must immediately notify a supervisor/manager in their chain of command (or other designated officials; e.g., CSOs or LSOs) of the incident.

2. However, time is of the essence and employees are not to delay reporting the incident to their supervisor/manager in order to obtain additional information.

3. If additional information becomes available after the initial report, it should be provided to the supervisor/manager (or other designated individuals) as soon as possible.

4. An employee's responsibility for reporting is met when the supervisor/manager (or

other designated official) has been informed.

5. The information and details about an incident are sensitive and should only be shared with those who have a need to know; e.g., local supervisor/manager or the CSO or LSO or in accordance with component policy.

6. There may be rare instances when an employee is unable to reach a manager (or other designated official) immediately.
    - Only in such cases is an employee authorized to report an incident directly to ensure reporting occurs within one hour.
    - If the SSA intranet is available, report the incident to the NNSC using the **PII Loss Reporting Tool** [redacted])
    - If the SSA intranet is not available, call SSA's NNSC directly at [redacted] to report the event. The NNSC is available 24 hours per day, 7 days per week, and 365 days per year.
        - See the PII Loss Worksheet (15.02.06) for the information that the NNSC will need.
        - NNSC personnel will take the report and provide a Change, Asset, and Problem Reporting System (CAPRS) number, which is to be provided to the supervisor/manager (or designated official).

7. In the situation above when an employee reports the incident directly, the employee is not authorized to use or apply the guidance in 15.02.04 and they should simply make the report. In those limited situations, component and/or central office staff involved in PII reporting will evaluate the situation and take appropriate action.

E. **Manager Procedures**

1. Managers (and for purposes of this section this includes designated employees (e.g., CSO, LSO, COTR POC)) must accept the incident report and are primarily responsible for reporting the loss or suspected loss of PII to the NNSC.

2. They should evaluate the incident using the guidance provided in 15.02.04 to determine if it warrants reporting to the NNSC.

3. Reports to the NNSC are to be made immediately, but no later than one hour of being notified of the incident.
    - If the SSA intranet is available, report the incident to the NNSC using the **PII Loss Reporting Tool** [redacted]
    - If the SSA intranet is not available, report the incident by contacting the NNSC at [redacted]. The NNSC is available 24 hours per day, 7 days per

week, and 365 days per year.

- See the PII Loss Worksheet (15.02.06) for the information that the NNSC will need.
- NNSC personnel will take the report and provide a Change, Asset, and Problem Reporting System (CAPRS) number, which is to be retained.
- Once access to the intranet is possible, return to the PII Reporting Tool site and, using the previously provided CAPRS number, update that system with the facts of the incident.

4. In addition to making the report, managers must follow any approved component level directives. This may include additional actions or notifications to the CSO or LSO, or a fact sheet or incident report to the component PII loss contact.
5. Managers are reminded to take any necessary agency or component actions such as filing a:
   - Police Report for stolen items;
   - Incident report through the Automated Incident Reporting System (AIRS) in SAFE[1];
   - SSA-342 for SSA property with an SSA inventory barcode or an acquisition value of $1000 or more[2];
   - NNSC CAPRS ticket for replacement of equipment; and/or
   - Report with the Office of the Inspector General (OIG), including PII incidents:
     - Involving the PII of an Individual of Extraordinary National Prominence (IENP).
     - Involving the loss of any correspondence from an SSA facility that was addressed to members of the public and/or agency employees prior to it being accepted by the USPS.
     - Involving the loss of electronic media (i.e., USB drive, CD/DVD, etc.).
     - Involving 50 or more individuals.

NOTE: The PII Loss Reporting Tool will copy the incident report to the OIG if the initial incident report contains any indication of theft or law enforcement involvement, loss of electronic media or if 50 or more individuals are involved. If these aspects are not included on the initial report but are identified afterwards (or any case involving IENP), then the manager handling the incident should notify the OIG by sending the PII or CAPRS number and a copy of the incident report to [redacted]@ssa.gov .

15.02.05 Management Evaluation of PII Incidents

[redacted]

15.02.06 Clarification on Losses Caused by Shipping Incidents

SSA is responsible for reporting PII incidents resulting from items being lost while being shipped or mailed. In these situations, SSA will usually be notified of the incident by the shipper. In general, the sending party (the party making the shipment) should report the incident. However, incidents involving agency mail (including checks mailed by the Treasury) that occur within the control of the United States Postal Service (USPS) are reported by and investigated by the USPS and therefore do not have to be reported by SSA. Incidents that occur after the addressee has received the material are the responsibility of the addressee.

[1] AIMS Guide GAM 10.05.03, Automated Incident Reporting System (AIRS)

[2] AIMS Guide MRM 04.05, Reporting Lost, Stolen, or Damaged SSA Controlled Personal Property

[3] M 07 16 Agencies should use a best judgment standard to develop and implement a breach notification policy. Using a best judgment standard, the sensitivity of certain terms, such as personally identifiable information, can be determined in context. For example, an office rolodex contains personally identifiable information (name, phone number, etc.). In this context the information probably would not be considered sensitive; however, the same information in a database of patients at a clinic which treats contagious disease probably would be considered sensitive information. Similarly, using a best judgment standard, discarding a document with the author's name on the front (and no other personally identifiable information) into an office trashcan likely would not warrant notification to US CERT.

15.02.07 Attachments

Attachments: Worksheet for Reporting Loss or Potential Loss of PII

Logging Is Required When PII Leaves SSA Workplace

Manual/Chapter: General Administration » Personally Identifiable Information (PII) Loss and Remediation
Instruction/Handbook: GAM 15.03
Audience: General
Level: SSA
Inquiries: Office of Privacy and Disclosure (OPD) | [redacted]@ssa.gov | 410 966 6645
Related Instructions: Office Of The General Counsel (OGC) » Office of Privacy and Disclosure (OPD)
Updated: 8/4/2020
Certified: *(not yet certified)*

Table of Contents

15.03.01 Purpose of Instruction

A. OMB M 06 16 requirement applicable to all agencies: Log all computer readable data extracts from databases holding sensitive information and verify each extract including sensitive data has been erased within 90 days or its use is still required.

B. This instruction provides agency policies and requirements that implement the requirement of OMB M-06-16 that agencies log data extracts. This instruction governs the logging of PII that will leave agency workspace either because:

1. it is being released to a third party or
2. it is being taken out of the workspace by employees (or contractors, subcontractors, or grantees) in performance of their official duties.

In developing this policy, SSA considered its business needs and existing security controls in order to identify areas for which there is reasonable risk of data loss or misuse.

C. Logging ensures appropriate management oversight, safeguards, and controls are applied prior to PII to leaving SSA's secure environment. It ensures that in the event that a loss occurs (or is suspected) the agency has sufficient information to compile a complete list of those potentially affected. This information is needed both to quantify the extent of the loss and enable the agency to notify the affected people, if necessary.

D. Publication of this AIMS guide codifies and supersedes all prior agency guidance and replaces the following memos: "Memo for Safeguarding Personally Identifiable Information (PII) While In Transit or Outside of Secure SSA Space" dated March 5, 2007 (Superseded) "Safeguarding Personally Identifiable Information (PII) While in Electronic or Physical Transit or Outside of Secure SSA Space " dated January 1, 2008 and "Safeguarding Personally Identifiable Information (PII) While in Transit or Outside of Secure SSA Space" dated February, 2008. "Procedures for Safeguarding Personally Identifiable Information (PII) While In Transit or Outside of Secure SSA Space" dated March 5, 2007, "Transporting Electronic Files Containing Personally Identifiable Information (PII) Outside of SSA" dated January 1 2008 and "Transporting Electronic Files Containing Personally Identifiable Information (PII) Outside of SSA" dated February, 2008.

15.03.02 Authorities and References

A. *Privacy Act of 1974* as amended (5 U.S.C. 552a) (Privacy Act of 1974)

B. OMB Memo M 06 15, Safeguarding Personally Identifiable Information, May 22, 2006

C. OMB Memo M 06 19, Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments, July 12, 2006

D. Recommendations for Identity Theft Related Data Breach Notification, September 20, 2006

E. OMB Memo M-06-16, Protection of Sensitive Agency Information, June 23, 2006

F. OMB Memo M 07 16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, May 22, 2007

G. Federal Information Processing Standards Publication 199: Standards for Security Categorization of Federal Information and Information Systems

H. The Federal Information Security Management Act (FISMA) of 2002, 44 U.S.C. § 3541

I. Information Security Policy (ISP)

J. National Institute of Standards and Technology (NIST) Special Publication 800 122 Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)

K. M-15-01, Fiscal Year 2014-2015 Guidance on Improving Federal Information Security and Privacy Management Practices

15.03.03 Background

PII can legitimately leave an SSA facility primarily in two ways:

1. It leaves an SSA facility because it is being released to a third party who has been authorized to have the data; or
2. It leaves an SSA facility in the custody of an SSA employee (contractor, subcontractor or grantee) that will be using it off-site for official agency business.

While similar, each situation has its own rules regarding logging and exceptions.

15.03.04 Release of Information to Third Parties - Logging Policy

A. Longstanding agency disclosure policy requires compliance with federal law and regulation before SSA employees and contractors, subcontractors or grantees may release SSA information to third parties (see AIMS, GAM 14.01.01).

B. Effective January 1, 2008, if SSA employees are releasing information containing PII (categorized per Federal Information Processing Standards 199 as moderate to high impact) to third parties outside of SSA's secure environment (see AIMS, GAM 15.01), then that material must be logged prior to transmission or release to the third party.

C. Additionally, within 90 days of release of the information, the following must be verified:

   1. That the data has been returned; or
   2. That the data has been erased or otherwise destroyed; or
   3. That continued use is still required (and that a new due date for return (or

destruction) of the information is established).

D. Log files should be retained in accordance with agency records retention (AIMS, MRM, Records Management Handbook - Chapter 1) and security policy. For these logs, that means a 2 year retention unless the log is relevant to a PII incident, in which case the material should be retained for 7 years. See also AIMS, GAM 15.04 for encryption policy that may also be applicable in this situation.

15.03.05 Release of Information to Third Parties - Logging Policy Exceptions

A. The policy in 15.03.03 does not apply to the following exceptions, which have been developed based upon assessment of risk:

1. Data moving solely within SSA's secure environment or to data transmitted to an external Trusted System. (See AIMS, GAM 15.01 for definitions.)

   NOTE: Data within SSA's secure environment is already subject to stringent access controls, security standards and requirements as well as business controls and audit oversight. Therefore, it is subject to a much lower risk of being lost or misused than data that leaves the SSA secure environment.

2. Providing information in response to individual or group requests for information containing PII when the disclosure is made under a provision of applicable law, such as the release of information that is provided to the subject of the information, to a third party that possesses written consent authorizing release of the information, to the U.S. Courts or other tribunals, or to law enforcement for purposes consistent with Agency disclosure policies.

B. If logging is not required, see AIMS, GAM 15.04 for encryption policy that might still be applicable.

15.03.06 Release of Information to Third Parties - Procedure

A. The SSA component that approves the release of the data to the third party must complete a log that meets the minimum file requirements listed in 15.03.06.

B. This requirement is deemed satisfied if a request for electronic access to agency data containing PII is conducted in accordance with existing agency policy (i.e., disclosure, privacy and/or data exchange), and is in the form of a formal agreement that requires compliance to the same laws and/or regulations or equivalent standards to which SSA must comply (i.e., FISMA , Privacy Act , Computer Matching and Privacy Protection Act, Federal Acquisition Rules, OMB directives, SSA security rules, compliance and auditing requirements). (See Information Exchange and Matching if a formal data exchange is involved.)

15.03.07 Release of Information to Third Parties - Minimum Log File Requirements

A. There is no SSA standardized form for logging the release of PII to third parties.

B. Components are free to use whatever form or format or to require additional information (i.e., encryption status) as long as the log contains at least the following items:

1. The name of the organization receiving the file or document;
2. The name of the component preparing the file or document;
3. The name of the file or document containing PII;
4. The date the file or document containing PII leaves SSA;
5. The date that the file or document containing PII is to be returned;
6. The date the file or document containing PII is:
   - actually returned to SSA or
   - is verified as erased/destroyed.
7. If appropriate:
   - the date the SSA manager approves retention of the file or document beyond 90 days,
   - the approving official's name, component and phone number and
   - the new due date for return of that file or document to SSA or
   - the verified destruction date of the file or document containing PII.

15.03.08 Removal of PII from the Workspace - Logging Policy

A. Effective January 1, 2008, SSA employees (or contractors, subcontractors or grantees) must have supervisory approval and comply with the logging requirements of this policy when removing files or documents containing PII (categorized per Federal Information Processing Standards 199 as moderate to high impact) that are:

1. Printed on paper or extracted from an SSA system; or
2. Copied to a portable media device such as a laptop, Compact Disc (CD), Digital Video Disc (DVD), flash-drive, or personal digital assistant; and
3. Physically removed outside of SSA's secured, physical perimeter (this includes being transmitted electronically (i.e., using email) to non SSA destinations).

B. Once that approval has been given, the material that will be taken from the workplace must be logged out by the employee/contractor. The supervisor manager is to verify that that it has been returned or erased/destroyed within 90 days of removal. (The 90 day timeframe can be extended if the supervisor/ task manager agrees that ongoing use of the data is still required and sets a new return date.)

C. Log files should be retained in accordance with agency records retention and security policy. For these logs, that means a 2-year retention unless the log is relevant to an incident, in which case the material should be retained for 7 years. See also AIMS, GAM 15.04 for encryption policy that may also be applicable in this situation.

D. Examples of situations when this policy would apply are situations such as work at home or working at an alternative duty station and official travel.

15.03.09 Removal of PII from the Workspace - Procedure

A. Before files or documents containing PII can be removed, managers must approve the removal. Employees must record the specific information required in 15.03.09 in a log maintained by the manager. Immediately upon returning to the official duty station, employees must log the return or disposition of the file(s) or document(s).

B. Managers must provide employees with contact information and instructions to be used in the event of a loss or suspected loss of PII and monitor the log file.

C. Material being removed must still be protected in accordance with agency policies (see AIMS, GAM 15.04.01 for encryption policy that may also be applicable).

15.03.10 Removal of PII from the Workspace - Minimum Log File Requirements

A. There is no SSA standardized form for logging PII leaving the workspace.

B. Components are free to use whatever form or format or to require additional information (i.e., encryption status) as long as the log contains at least the following items (Self reporting):

1. The name of the employee removing the file or document;
2. The name of the file or document containing PII;
3. The reason for removal;
4. The date the file or document containing PII leaves SSA;
5. The date that the file or document containing PII is to be returned;
6. The date the file or document containing PII is

- actually returned to SSA or
- is verified as erased/destroyed.

7. If appropriate:
    - the date the SSA manager approves retention of the file or document beyond 90 days,
    - the approving official's name, component and phone number and
    - the new due date for return of that file or document to SSA or
    - the verified destruction date of the file or document containing PII.

Mandatory Encryption of Electronic Data on Mobile Computers and Devices

Manual/Chapter: General Administration » Personally Identifiable Information (PII) Loss and Remediation
Instruction/Handbook: GAM 15.04
Audience: General
Level: SSA
Inquiries: Office of Privacy and Disclosure (OPD) | [redacted]@ssa.gov | 410 966 6645
Related Instructions: Office Of The General Counsel (OGC) » Office of Privacy and Disclosure (OPD)
Updated: 2/3/2025
Certified: 2/3/2025

Table of Contents

15.04.01 Purpose of Instruction

1. OMB M-06-16 requirement applicable to all agencies: "Encrypt all data on mobile computers/devices which carry agency data unless the data is determined to be non sensitive, in writing, by your Deputy Secretary or an individual he/she may designate in writing."

2. This instruction provides agency policies and requirements regarding how SSA implements this directive. This includes email.

15.04.02 Authorities and References

1. *Privacy Act of 1974* as amended (5 U.S.C. 552a) (Privacy Act of 1974)
2. OMB Memo M-06-15, Safeguarding Personally Identifiable Information, May 22, 2006
3. OMB Memo M-06-19, Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments, July 12, 2006
4. Recommendations for Identity Theft Related Data Breach Notification, September 20, 2006
5. OMB Memo M 06 16, Protection of Sensitive Agency Information, June 23, 2006
6. OMB Memo M 07 16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, May 22, 2007
7. Federal Information Processing Standards Publication 199: Standards for Security Categorization of Federal Information and Information Systems
8. The Federal Information Security Management Act (FISMA) of 2002, 44 U.S.C. § 3541
9. Information Security Policy (ISP)
10. National Institute of Standards and Technology (NIST) Special Publication 800-122 - Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)
11. M 15 01, Fiscal Year 2014 2015 Guidance on Improving Federal Information Security and Privacy Management Practices

15.04.03 Background

Note that encryption is a tool that was already incorporated into SSA's enterprise security posture prior to publication of OMB M 06 16, and those decisions and processes regarding encryption remain in effect. M-06-16 provides agencies with additional reasons to roll out or improve encryption at the enterprise. The following directives are not aimed at the enterprise; they are aimed primarily at securing electronic data on laptops and other electronic devices, portable electronic media and email. Physical security of these same resources is addressed under existing resource protection policies.

15.04.04 Encryption Policy

A. Encryption is a security technique applicable only to electronic devices or to data in electronic format.

B. The following are mandatory agency policies:

1. Agency laptops must be encrypted.
2. All data on electronic media and memory devices (i.e., DVD, CD, flash drive) must be encrypted.
3. PII being transmitted electronically (i.e., via email or other approved electronic method) must be encrypted.

C. See also AIMS, GAM 15.03.01 for logging policies that may apply to such data.

15.04.05 Encryption Policy Exceptions

[redacted]

[redacted]

15.04.06 Encryption Procedure

A. **Laptops**
This agency policy is being implemented using enterprise software. The agency encryption solution for laptops is called SecureDoc [1] and the Office of Chief Information Officer has procured solutions for the vast majority of laptops owned by the agency. Technical instructions for installing this software can be found at [redacted]

B. **Electronic Media**
The Office of Chief Information Officer has procured an encryption solution for removable media called Removable Media File Encryption (RMFE). [2] [3] It will encrypt media containing sensitive data that is transported or stored off site. This includes but is not limited to USB flash drives, CDs, DVDs, or floppies containing sensitive information. If encryption of the media itself is not possible, it is acceptable to encrypt the data that is being placed on the media. This can be done using WinZip (ISP 3.3.5 Secure Email Use Policy). If the agency business process that produces CDs or DVDs does not (yet) encrypt them automatically, then unencrypted CDs must be password-protected. [4]

C. **Email**
As SSA's email system is encrypted for internal use, email that goes to and from an ssa.gov address does not require additional encryption. See 15.04.06 for additional information on email.

D. **Fax**
Encryption is not mandatory for FAX, see ISP 3.3.5 Secure Email Use Policy .

E. **Other Electronic Transmission Methods**
There are currently no other approved electronic transmission methods. This will be updated as other technologies are approved.

15.04.07 Additional Procedures Related to Using Email (or Other Approved Methods) to Send PII

A. SSA has extended the encryption requirements in OMB M-06-16 to include data that is transmitted electronically (i.e., via email or other approved electronic communication

methods).

B. Limits to PII that can be included in an unencrypted email sent by:

1. An employee.

A. Name - the recipient's name

B. Request for Information - i.e. birth certificates, marriage certificates, additional forms and/or information required for the claim, etc.

C. SSA representative contact Information i.e. claims representative's name, phone number, field office address, etc.

2. An agency business process (i.e., iAppeal, iClaims, MySSA etc). Agency business processes that want to communicate via email with a claimant or members of the public can do so only after such communications are reviewed and documented in accordance with existing agency policies for compliance with privacy, disclosure and PII protection requirements.

C. See ISP 3.3.5 Secure Email Use Policy . for detailed procedures on how to send email securely.
NOTE: Advise the individuals being contacted to not send SSA their personal information via unsecure email in response to our emailed requests.
NOTE: Consider alternatives to email, such as the Government Services Online (GSO) portal if available. Staff in the Office of Electronic Services and Technology (OEST), DCO can provide more information about GSO capabilities.

15.04.08 Related Policies

At all times, but particularly when encryption is not possible, the following related physical security directives must be always be followed (see AIMS, MRM 04.50.01, SSA Physical and Protective Security Program).

1. PII stored on portable electronic media that cannot be encrypted or in hard copy must be kept physically secure, e.g., stored in a locked compartment, such as filing cabinet or desk drawer when not in use.

2. When transporting PII, you must make every reasonable effort to secure and lock the materials in a locked trunk, brief case, or other lockable device during transport. Do not leave them in the passenger compartment.

3. After you reach your destination, do not leave PII in the vehicle but securely store them at your destination in the most secure manner available.

[1] See SecureDoc Documentation: [redacted]

[2] Contact SSA's Information Center for additional information:
[redacted]

[3] File and Removable Media Protection (FRP) Home

[4] ISP Section 6.3 Encryption Policy: ISP: Section III Protect | OIS

Executive Oversight of PII Loss Notification and Remediation Policy and Process

Manual/Chapter: General Administration » Personally Identifiable Information (PII) Loss and Remediation
Instruction/Handbook: GAM 15.05
Audience: General
Level: SSA
Inquiries: Office of Privacy and Disclosure (OPD) | [redacted]@ssa.gov | 410 966 6645
Related Instructions: Office Of The General Counsel (OGC) » Office of Privacy and Disclosure (OPD)
Updated: 7/17/2020
Certified: *(not yet certified)*

Table of Contents

15.05.01 Purpose of Instruction

A. OMB M 07 16 requirement applicable to all agencies: "To ensure adequate coverage and implementation of the plan, each agency should establish an agency response team including the Program Manager of the program experiencing the breach, Chief Information Officer, Chief Privacy Officer or Senior Official for Privacy, Communications Office, Legislative Affairs Office, General Counsel and the Management Office which includes Budget and Procurement functions."

B. This section documents the agency's executive management oversight regarding PII loss notification and remediation policy and practice. This AIMS guide codifies and

supersedes all prior agency guidance.

15.05.02 Authorities and References

A. *Privacy Act of 1974* as amended (5 U.S.C. 552a) (Privacy Act of 1974)

B. OMB Memo M 06 15, Safeguarding Personally Identifiable Information, May 22, 2006

C. OMB Memo M 06 19, Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments, July 12, 2006

D. Recommendations for Identity Theft Related Data Breach Notification, September 20, 2006

E. OMB Memo M-06-16, Protection of Sensitive Agency Information, June 23, 2006

F. OMB Memo M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, May 22, 2007

G. Federal Information Processing Standards Publication 199: Standards for Security Categorization of Federal Information and Information Systems

H. The Federal Information Security Management Act (FISMA) of 2002, 44 U.S.C. § 3541

I. Information Security Policy (ISP)

J. National Institute of Standards and Technology (NIST) Special Publication 800 122 Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)

K. M-15-01, Fiscal Year 2014-2015 Guidance on Improving Federal Information Security and Privacy Management Practices

15.05.03 Background

A. The Commissioner of Social Security (COSS) is the final decision maker regarding SSA PII loss notification and remediation policy. The PII Incident Response Group (IRG), assists the COSS by providing oversight and recommendations on agency PII loss notification and remediation policy. The IRG also ensures implementation of the Breach Notification Policy and plan.

B. Directives from OMB require all Federal agencies to identify a core management response group whose role is to engage in agency planning in the event of a breach. To comply with OMB's directive, the agency has appointed the agency Chief Information Security Officer as the PII Incident Coordinator and established the IRG.

15.05.04 Administrative Support

Office of Chief Information Officer (OCIO) provides basic administrative support for the IRG.

15.05.05 Attachments

Attachments: Incident Response Group Charter
Incident Response Process Flow

SSA Breach Notification Plan (BNP)

Manual/Chapter: General Administration » Personally Identifiable Information (PII) Loss and Remediation
Instruction/Handbook: GAM 15.06
Audience: General
Level: SSA
Inquiries: Office of Privacy and Disclosure (OPD) | [redacted]@ssa.gov | 410 966 6645
Related Instructions: Office Of The General Counsel (OGC) » Office of Privacy and Disclosure (OPD)
Updated: 7/17/2020
Certified: *(not yet certified)*

Table of Contents

15.06.01 Purpose of Instruction

A. OMB M 07 16 requirement applicable to all agencies: "Each agency should develop a breach notification policy and plan comprising the elements discussed in this

Attachment. In implementing the policy and plan, the Agency Head will make final decisions regarding breach notification.

B. The purpose of the Breach Notification Plan (BNP) is to establish a framework for when and how agencies will notify the subject of a harmful breach. The BNP and related procedures will ensure that SSA takes a consistent, reasonable approach to remediation and notification when there is a loss or suspected loss of PII. Publication of this AIMS guide codifies and supersedes all prior agency guidance.

15.06.02 Authorities and References

A. *Privacy Act of 1974* as amended (5 U.S.C. 552a) (Privacy Act of 1974)

B. OMB Memo M-06-15, Safeguarding Personally Identifiable Information, May 22, 2006

C. OMB Memo M-06-19, Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments, July 12, 2006

D. Recommendations for Identity Theft Related Data Breach Notification, September 20, 2006

E. OMB Memo M 06 16, Protection of Sensitive Agency Information, June 23, 2006

F. OMB Memo M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, May 22, 2007

G. Federal Information Processing Standards Publication 199: Standards for Security Categorization of Federal Information and Information Systems

H. The Federal Information Security Management Act (FISMA) of 2002, 44 U.S.C. § 3541

I. Information Security Policy (ISP)

J. National Institute of Standards and Technology (NIST) Special Publication 800-122 - Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)

K. M 15 01, Fiscal Year 2014 2015 Guidance on Improving Federal Information Security and Privacy Management Practices

15.06.03 Background

The Privacy Act , the E Government Act of 2002 (including FISMA) , and OMB guidelines, including M-07-16 , are the foundation of our BNP. Our BNP describes how we assess whether individuals are at risk of harm due to the breach, and whether we should provide notice of the breach to individuals and/or the public. The SSA BNP is distinct from OMB Guidance and our policy pertaining to reporting the loss of PII to management or to organizations such as the US Computer Emergency Response Team (US-CERT), which are covered by existing directives (see AIMS, GAM 15.02). The SSA BNP does not replace existing policy and procedure regarding security protocols and requirements for handling a security incident (see the Information Security Policy (ISP)).

15.06.04 Scope

This policy is applicable agency-wide. It is one component of our comprehensive policies and procedures applicable to safeguarding information, implementing Privacy Act provisions, and responding to the loss of PII. The concept of the BNP is to use a best judgment standard, e.g., the sensitivity of a PII loss will be determined in context, to determine if risk of harm exists as a result of the breach. If risk of harm exists, notification may help individuals take steps to protect themselves from the consequences of the breach.

15.06.05 Policy

A. The Deputy Commissioner or equivalent level official is responsible for ensuring that the component responds to the PII breach in accordance with this policy. The component that experiences the breach will work in consultation with the PII Breach Response Group (BRG). (See AIMS, GAM 15.05.)

B. SSA's BNP requires the agency Incident Response Group (AIMS 15.05) to determine if a breach of PII puts an individual at risk of harm. To determine if we should notify affected individuals, the BNP requires us to consider the likely risk of harm and the level of impact. Our analysis of the likely risk of harm and the level of impact will determine when, what, how, and who we should notify.

C. If the breach involves an information system, SSA will follow existing procedures to take steps to mitigate further compromise of the system(s) involved in a breach. In addition to containing the breach, if circumstances warrant, we will take appropriate countermeasures, such as monitoring system(s) for misuse of the PII and for patterns of suspicious behavior. We also may consider whether we should give notice to the public at large.

D. In deciding whether to provide notice, we should give greater weight to the likelihood that the PII is accessible and usable and to the likelihood that the breach may lead to harm. If we analyze the factors (see "Factors to Consider" below) in a fact specific context, it is likely that we only will provide notification in instances where there is a likely risk of harm.

15.06.06 Is There Likely Risk of Harm – Factors to Consider

A. The decision-maker is to consider the specific facts, circumstances, and the context of the breach to evaluate the likely risk of harm and the level of impact on the individual(s). The decision-maker will use this information to determine whether notice should be given and to determine the nature and extent of the notice.

B. However, the fact that information has been lost or stolen does not necessarily mean it has been or can be accessed by unauthorized individuals. If information is properly protected (e.g., consistent with NIST standards and guides) the risk of compromise of the information may be low to non existent.

15.06.07 Factors that Determine the Risk of Harm

A. **Nature of the Data Elements Breached.**
Identify the type of data breached. We consider the data elements in light of their context and the broad range of potential harms that may result from their potential use by unauthorized individuals.

B. **Number of Individuals Affected.**
The number of individuals affected is not determinative of the risk of harm. We will consider the number of affected individuals when determining the type or method(s) we use to provide notification.

C. **Can an Unauthorized Person Access the Information?**
We use NIST "Level of Impact" guidelines (see Definitions, 15.01) and consider answers to the questions below to assess the likelihood the breached information is accessible and will be used for malicious purposes.

1. Circumstances of the loss. How did the loss occur? Is the loss the result of a criminal act or is it likely to result in harm to the individual?

2. How easy or difficult is it to access the information in light of how the information is protected? For example, information on a protected (i.e., encrypted) device is less vulnerable than "hard copies" and unencrypted devices and files.

3. Is there evidence that the breached information is being used to harm the individual?

4. What is the likelihood unauthorized individuals will know the value of the information or sell it to others?

D. **Can the Information Be Used to Cause Harm to Individuals?**

1. **Broad Reach of Potential Harm.** The Privacy Act requires agencies to protect against any anticipated threats or hazards to the security or integrity of records which could result in "substantial harm, embarrassment, inconvenience, or

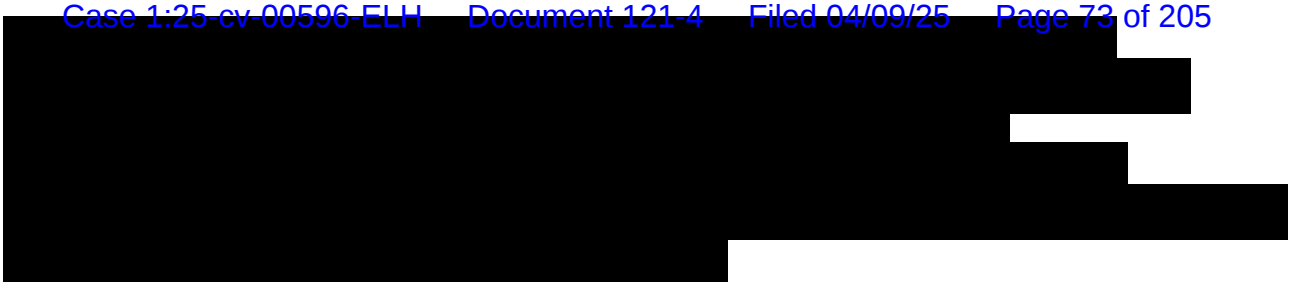
unfairness" to any individual on whom information is maintained. SSA considers a number of possible harms associated with the breach of information:

- Economic Identity Theft;
- Medical Identity Theft;
- Theft;
- The effect of a breach of confidentiality on fiduciary responsibility;
- The potential for blackmail;
- The disclosure of private facts;
- Mental pain and emotional distress;
- Physical harm, e.g., disclosure of address information for victims of abuse;
- The potential for secondary uses of the information which could result in fear or uncertainty for the subject individuals; and/or
- The unwarranted exposure of information leading to humiliation or loss of self-esteem.

2. **Likelihood Harm Will Occur.** We ascertain if the type of information breached typically is used to cause harm to individuals. We may consult with law enforcement and/or the Office of the Inspector General (OIG) to assess the risk of harm to the individual.

   After evaluating these factors, we review and reassess the level of impact (not low, low, moderate or high) that previously we assigned to the information using the NIST impact levels. The NIST impact levels (see Definitions, 15.01) will determine when and how we should provide notification.

15.06.08 Whether Breach Notification Is Required



15.06.09 Content of Notification

A. We will use plain language. We will include the following information in all our breach notification materials, regardless of the medium or method.

B. An apology;

C. A brief description of what happened, including the date(s) of the breach and the date that we discovered it;

D. A description of the types of PII involved in the breach (e.g., full name, Social Security number, date of birth, home address, disability information);

E. A statement whether the information is protected;

F. What steps individuals might wish to take to protect themselves from potential harm;

G. What we are doing to investigate the breach, to mitigate losses, and to protect against any further breaches; and

H. Who affected individuals should contact for more information, which may include a toll free telephone number, and/or postal address.

15.06.10 SSA Official Responsible for Notification

A. The COSS or his/her designee will sign the written notices that we send to individuals. Notification must be compliant with Section 508 of the Rehabilitation Act. The law may require us to establish a Telecommunications Device for the Deaf (TDD) and/or to post a large print notice on the Agency's web site.

B. If the breach involves a Federal contractor or a public private partnership operating a system of records on our behalf, we will determine who is responsible for notification and ensure that corrective actions are taken. We include appropriate Federal Acquisition Regulation language regarding Federal Information Security Management Act requirements and PII loss reporting responsibilities in all contracts and other acquisition documents.

15.06.11 How SSA Provides Notice

As stated in 15.06.07, in general breach notifications to individuals will be by letter or by telephone. The best means for providing notification will depend on the number of individuals affected and what contact information is available about the affected individuals. Notice provided to individuals affected by a breach should be commensurate with the number of people affected and the urgency with which they need to receive notice. The following examples are types of notices that we may use.

NOTE: The Office of Budget, Finance, Quality, and Management , the Office of Legislative and Congressional Relations and Office of General Counsel/Office of Privacy and Disclosure must be consulted when preparing a notice (other than the one in Attachment Sample PII Breach Notification Letter); likewise any component considering web posting, existing government wide services, newspapers or other public media outlets or substitute notice must confer with these offices as part of the development of the product.

A. **Telephone:** Telephone notification may be appropriate in those cases where urgency may dictate immediate and personalized notification and/or when a limited number of individuals are affected.

B. **First-Class Mail:** We will provide written notice by first-class mail. We will send the notice separately from other SSA mailings so that it is obvious to the recipient that it pertains to SSA and that the matter is urgent.

C. **E Mail:** We may use e mail notification exclusively only if the individual has provided an e-mail address to us and expressly has given his or her consent to use e-mail as the primary means of communication with us. We may use e mail in conjunction with written notice if the circumstances of the breach warrant such an approach. E-mail notification may include links to the Agency and http://www.usa.gov/ web sites, where the notice may be "layered" so that the most important summary facts are up front with additional information provided under link headings.

D. **Web Posting:** Depending on the circumstances, we may post information about the breach and notification on our home page. The posting may include a link to Frequently Asked Questions (FAQs) and other information to assist the public's understanding of the breach and of the notification process. The information also may appear on the http://www.usa.gov/ web site. We may consult with the General Services Administration's (GSA) USA Services regarding using their call center.

E. **Existing Government Wide Services:** We may consider Government-wide services already in place to provide support services such as USA Services, including 1 800 FedInfo and http://www.usa.gov/ .

F. **Newspapers or other Public Media Outlets:** In rare circumstances, we may supplement individual notices with notifications in newspapers or other public media outlets. We may use toll-free call centers staffed by trained personnel to handle inquiries from the affected individuals and the public.

G. **Substitute Notice:** We may use substitute notice in those instances where we do not have sufficient contact information to provide another means of notification. Substitute notice may consist of a conspicuous posting of the notice on the home page of our web

site and/or notification to major print and broadcast media, including major media in areas where the affected individuals reside. The notice to media may include a toll-free phone number where an individual can learn whether or not his or her personal information is included in the breach.

15.06.12 Attachment

Attachments: Sample PII Breach Notification Letter

Agency Compliance with Specific OMB Directives Related to PII

Manual/Chapter: General Administration » Personally Identifiable Information (PII) Loss and Remediation
Instruction/Handbook: GAM 15.07
Audience: General
Level: SSA
Inquiries: Office of Privacy and Disclosure (OPD) | [redacted]@ssa.gov | 410 966 6645
Related Instructions: Office Of The General Counsel (OGC) » Office of Privacy and Disclosure (OPD)
Updated: 3/15/2021
Certified: 3/15/2021

Table of Contents

15.07.01 Purpose of Instruction

A. OMB M 07 16 requirement applicable to all agencies: "Ensure all individuals with authorized access to personally identifiable information and their supervisors sign at least annually a document clearly describing their responsibilities. Therefore, it is the responsibility of each agency head to develop and implement an appropriate policy outlining the rules of behavior and identifying consequences and corrective actions available for failure to follow these rules."

B. This instruction provides agency policies and requirements regarding how SSA implements this directive. The information in this chapter provides guidance to managers on key responsibilities and is intended to supplement, but not replace, existing agency or component directives covered in other agency directives.

15.07.02 Authorities and References

A. *Privacy Act of 1974* as amended (5 U.S.C. 552a) (Privacy Act of 1974)

B. OMB Memo M-06-15, Safeguarding Personally Identifiable Information, May 22, 2006

C. OMB Memo M-06-19, Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments, July 12, 2006

D. Recommendations for Identity Theft Related Data Breach Notification, September 20, 2006

E. OMB Memo M 06 16, Protection of Sensitive Agency Information, June 23, 2006

F. OMB Memo M 07 16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, May 22, 2007

G. Federal Information Processing Standards Publication 199: Standards for Security Categorization of Federal Information and Information Systems

H. The Federal Information Security Management Act (FISMA) of 2002, 44 U.S.C. § 3541

I. Information Security Policy (ISP)

J. National Institute of Standards and Technology (NIST) Special Publication 800-122 - Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)

K. M 15 01, Fiscal Year 2014 2015 Guidance on Improving Federal Information Security and Privacy Management Practices

15.07.03 Background

A. SSA's policies governing PII do not exist in isolation, but work alongside other agency policies that also have the effect of supporting the directive to protect PII. For example, a question about PII could touch upon or require familiarity with issues and existing agency policies and procedures in areas pertaining to privacy, information technology (IT) security, physical security, the Freedom of Information Act, the Privacy Act , records retention and records management. Administrative policies such as resource management and property disposal and human resource issues such as Telework, labor agreements and the roles and duties of employees and managers under applicable federal law and regulation could also be PII related or have an impact on protecting PII.

B. While OS has the responsibility for agency policy and procedures regarding IT security and PII breach issues, the fact is that these policies are built upon, and depend upon, the existence of and familiarity with these other agency directives, policies, and procedures. This is very evident in the area of personnel policies that guides employees and managers.

15.07.04 Annual Reminder

It is an OMB requirement that each agency develop a Rules and Consequences Policy that all individuals with access to PII are to sign annually. In response to that requirement, we have developed the Annual Reminder on Safeguarding Personally Identifiable Information (PII) for SSA Employees and its accompanying Acknowledgement Statement. Managers and supervisors must see that each employee is asked to sign the Acknowledgement Statement annually and it should be maintained in the employee's SF-7B file.

15.07.05 Additional Key Management Responsibilities

In addition to the directives found in AIMS, GAM 15.01, managers and supervisors have other related duties and responsibilities that are fundamental to protecting PII. These include (but are not limited to):

A. Enforcement of SSA's Rules of Behavior

B. Protecting agency employees, facilities and resources in accordance with agency standards

C. Enforcement of Telework requirements

D. Enforcement of the SSA Sanctions Policy

15.07.06 Attachments

Attachments:

Distribution of the Annual Reminder for Safeguarding Personally Identifiable Information (PII) for SSA Employees
Instructions for Annual Distribution of the Annual Reminder on Safeguarding Personally Identifiable Information (PII)
Annual Reminder for Safeguarding Personally Identifiable Information (PII) for SSA Employees

Assess Security and Privacy Risks

What is it?

Security risk assessments are essential elements of the National Institute of Standards and Technology (NIST) Risk Management Framework. Risk management involves identifying threats and vulnerabilities, estimating the likelihood of such threats exploiting vulnerabilities, determining the level of impact, recommending cost effective actions to mitigate or reduce risk, and documenting the assessment results. Digital Identity Risk Assessments (DIRA) (Formerly ARA) help federal agencies determine the degrees of confidence that they must have to engage in digital transactions with members of the public.

The Project Manager (PM), Security Authorization Manager (SAM), System Owner, Business Project Manager (BPM), Component Security Officer, Office of Privacy and Disclosure (OPD) Privacy Specialist, and Office of Information Security (OIS) are required to follow the risk assessment process to determine potential threats, vulnerabilities, and risks, identify appropriate controls to reduce and/or eliminate risks, and to present any residual risks to the Authorizing Official for acceptance.

The process of assessing security and privacy risks includes the completion of the following, as appropriate:

Privacy Assessments –Privacy assessments ensure that privacy controls selected by agencies are implemented correctly, operating as intended, and effective in satisfying security and privacy requirements and associated risk(s). PMs are required to provide OPD via email at [redacted] with:

- A description of the project;
- Any previous coordination with OPD regarding the project; and
- Downstream project-specific requirements (e.g., need for an Authorization to Operate).

Using this information, OPD will determine the appropriate privacy assessment for the project and with the support of the PM, SAM, BPM, and other stakeholders, conduct one of the following on the release:

Privacy Threshold Analysis (PTA) –The PTA serves as the agency's baseline analysis to determine if a release collects, maintains, stores/processes, or discloses Personally Identifiable Information (PII) and is subject to requirements set forth by the Office of Management and Budget (OMB), the National Institutes of Standards and Technology (NIST), the Privacy Act, or the E-Government Act of 2002.

Privacy Impact and Risk Assessment (PIRA) –The PIRA is a comprehensive assessment of a system, application, or a project to ensure all identified and selected privacy controls have been implemented and that any identified privacy risks are adequately managed. PIRAs are required for systems, applications, or projects seeking an Authorization to Operate and must be reviewed and approved by the agency's Senior Agency Official for Privacy (SAOP), in accordance with OMB Circular A 130. See the Privacy Initiatives for Establishing an Authorization to Operate for more information.

Digital Identity Risk Assessment (DIRA) (Formerly ARA) –

A DIRA is required for all public-facing applications and automated telephone services (digital services).

The DIRA determines the required identity proofing, authentication, and federation security levels for digital services. The security levels are proportional to the negative impact bad actors could have if they were to successfully access digital services by compromising or stealing a credential or assertion of a legitimate user, or by receiving a credential or role issued to the wrong person.

The DIRA replaced the Authentication Risk Assessment (ARA) process in FY 2023 and is based on NIST Special Publication (SP) 800-63-3, Digital Identity Guidelines. All new digital services require a DIRA assessment prior to release, as do all subsequent releases that could result in a change in the risk to users or the agency. Not all DIRA requests result in a full assessment. In those cases where a full DIRA is required, the DIRA Team works closely with stakeholders to gather information and artifacts,

conducting a detailed analysis that culminates in a final DIRA Report. Project teams are encouraged to reach out to the DIRA Team early in the design phase for guidance and best practices related to digital identity.

Preliminary DIRA results are provided to project teams to support continued application development while the DIRA Report is in progress. The DIRA Report is a more comprehensive document that requires additional consultation and analysis and includes an overview of the application and business processes, related data transactions, a full digital identity impact assessment (including assessed assurance levels), relevant controls, recommendations and risk partner feedback, and resources used or considered during the assessment. The DIRA Report requires a thorough review and undergoes an approval process that culminates in ODT Associate Commissioner (AC)/Deputy Associate Commissioner (DAC) approval and storage in Xacta.

Interconnection Security Agreement (ISA) The ISA is a security agreement that specifies the technical and security requirements for planning, establishing, and maintaining an interconnection between SSA's information systems and external Federal entities.

Significant Change Determination Form (SCDF)- This form allows the security risk team to identify risk that will be added by this project entering the enterprise (Purchased services, purchased software, developed software, cloud usage, etc.). It may lead to the requirement of an authorization decision (ATO, ATU, etc.).

Is it required?

Risk assessments must be performed on all new or modified information systems (e.g. Security Authorization Boundary, Applications, and Sub-System/Components) as outlined in the Information Security Policy (ISP), Section 2.1 – Asset Management.

The completion of the following is required based on the conditions defined below:

A **PTA** is required for the first release of a project designated as Development (except for projects where the Infrastructure attribute in the Investment Management Tool (IMT) is Infra Architecture Support) or Cyclical. Subsequent releases require a review of the PTA by OPD. Contact [redacted] to determine if an updated or new PTA is required.

A **PIRA** is required instead of a PTA for information systems/applications undergoing an Authorization to Operate. When significant changes or

functionality enhancements to a previously authorized information system or application introduce new privacy compliance requirements or privacy risk(s), PMs, SAMs, BPMs, other stakeholders, and OPD must review and if necessary, update the existing PIRA. If a PIRA was not previously conducted, a new PIRA must be completed.

A **DIRA (Formerly ARA)** is required for the first release of any public-facing application or automated telephone service. It is also required for any significant change(s) to these services or as part of a periodic review.

Note: The DIRA cannot be waived.

An **ISA** is required if establishing an interconnection with an external Federal entity for releases designated as Development (except for releases where the Infrastructure attribute in IMT is Infra Architecture Support), Cyclical, or P&A Only. Complete the (attached) ISA Determination Form to determine if an ISA is needed.

An **SCDF** is required when changes to the enterprise are being made to information systems/applications or new information systems/applications are being added/developed/contracted. The SCDF is directly related to obtaining or maintaining an authorization decision.

When does it start/finish?

Not applicable

How is it done? (When applicable)

PTA: The PM contacts [redacted] to request a PTA or to review an existing PTA. The PTA is conducted by OPD with the assistance of the PM. OPD determines from the PTA if a new or amended PIA or SORN are required. OPD coordinates the drafting or revision of PIAs and SORNs with the PM and any other relevant stakeholders. OPD then stores the finalized PTA in a secured repository. The PM may send an email to ^OGC OPD Controls to request a copy of the finalized PTA and any necessary privacy related controls. The PIA and SORN, if required, are also stored by OPD and made available to the public on the SSA's public facing Privacy page.

PIRA: The PM contacts [redacted] to request a PIRA for an Authorization to Operate or to review an existing PIRA if significant changes

may result in the need for additional privacy controls or present new privacy risks. The PIRA is conducted by OPD with the assistance of the PM, SAM, BPM, and other stakeholders. OPD coordinates the review, approval, and signoff of the PIRA with the SAM, OPD Division Director for Privacy Compliance, OPD Executive Director, and the SAOP. The SAOP returns their approval and signature of the PIRA to OPD. OPD stores the finalized PIRA and SAOP decision memo in a secured repository with a copy of the PIRA provided to the SAM for purposes of providing it to the Authorizing Official.

Online DIRA (Formerly ARA) Request: The PM or their designee completes the Online DIRA (Formerly ARA) Request Form. Upon notification, the DIRA team will evaluate the submission and contact the project stakeholders to advise on next steps

ISA: Should an SSA component have a business need to establish a secure connection with SSA information systems and/or an external Federal entity, the PM, the BPM, and the SAM are responsible for working with internal stakeholders (e.g., OSOHE and OIS) to develop the ISA. Once the ISA is developed OIS approves and stores the artifact in a secured repository.

SCDF: Complete Significant Change Determination Form (SCDF)

IMT - Risks: The PM documents all risks in the Investment Management Tool (IMT).

Who participates?

- All stakeholders should be involved, (i.e., anyone who is providing something to or receiving something from the project).
- BPM
- CSO
- OPD Privacy Analyst
- Product Manager (PdM)
- Project Manager (PM)
- SAM
- System Owner

Work Templates

Significant Change Determination Form (JIRA ticket)

ISA Determination Form

Privacy Threshold Analysis (PTA)

Privacy Impact Risk Assessment (PIRA)

Online DIRA (Formerly ARA) Request Form

Who to Contact

CSO

[redacted]

Related Information

Information Security Policy (ISP) Section 2.1: Asset Management

DIRA (Formerly ARA) Business Process

Interconnection Approval Process

Personally Identifiable Information - Definitions

Investment Management Tool (IMT)

OMB Circular A 130 Privacy Protection Guidance

OMB Memorandum M-03-22, Guidance for Implementing Privacy Provisions of the E Government Act of 2002

Risk Management Framework

Web Application Security

Security Architecture Guide

Change History

Office of Information Security (OIS)

Information Security Officer Manual

Version 5.2

January 10, 2025

Revision History

Version	Revision Date	Brief Description	Author(s)	Last Reviewed Date	Reviewed / Approved by	Effective Date
2.1	06/17/2013	Document updates to including FY11 Assessment mitigations				
2.2	07/12/2013	Grammatical changes, updates to links				
2.3	07/25/2013	Formatting – No content change				
2.4	09/06/2013	Incorporated changes from CSO feedback				
2.5	07/01/2014	Grammatical changes; Formatting				
2.6	08/25/2014	Updated information, formatting, editing				

2.7	11/10/2014	Included Reason Code Section				
2.8	01/14/2015	Updated [redacted] Report Review and Certification Procedures				
2.9	01/15/2015	Overall edit and formatting revisions				
3.0	06/22/2015	Updated links, formatting, terminology revisions in Ch3 for clarification				
3.1	11/16/2015	Updated various links, format revisions, and procedural/terminology revisions relating to ISP (ISSH) and SAM (replaces form SSA-120)				
3.2	04/25/2017	Updated OTSO name change to OSOHE Updated [redacted] information Updated [redacted] information Updated [redacted] information Updated OIS organizational information and duties to reflect Realignment Updated AMB name change to SASSB				

		Updated OFSM name change to OFLM Removed outdated links, sections, exhibits.				
3.3	06/13/2017	Updated [redacted] Removed Section [redacted]				
3.4	03/06/2018	Updated SAM retention requirements in section 3.6.1-C from current 7 year requirement, to instead use NARA GRS Schedule 3.2				
3.5	06/14/2018	Defined the [redacted]				
3.6	07/20/2018	Clarified [redacted]				
3.7	08/23/2018	Link [redacted].				
3.8	02/14/2019	Updated all links and references to the Information Security Policy (ISP) to reflect restructured ISP.				

3.9	03/05/2019	Updated [redacted]				
4.0	04/08/2019	Updated [redacted]				
4.1	07/11/2019	Updated [redacted]				
4.2	10/21/2019	Corrected several broken links to SAM and OIS departments. Removed references to [redacted]	[redacted]	10/21/2019	[redacted]	10/21/2019
4.3	04/08/2020	Clarified [redacted]	[redacted]	04/07/2020	[redacted]	04/08/2020
4.4	04/10/2020	Corrected multiple broken links to ISP.	[redacted]	04/10/2020	[redacted]	04/10/2020
4.5	08/11/2020	Section [redacted]. Updated links to all AIMS references.	[redacted]	08/11/2020	[redacted]	08/11/2020
4.6	11/10/2020	Revised [redacted].	[redacted]	11/10/2020	[redacted]	11/10/2020

4.7	03/03/2021	Annual Review Completed. Updated links throughout.	[redacted]	03/03/2021	[redacted]	03/03/2021
4.8	09/16/2021	Updated [redacted]	[redacted]	09/16/2021	[redacted]	09/16/2021
4.9	10/19/23	Updated various sections across the entire documents.	[redacted]	10/19/2023	[redacted]	10/19/2023
5.0	03/28/2024	Removed [redacted] Updated [redacted]	[redacted]	02/16/2024	[redacted]	03/28/2024
5.1	06/14/2024	Removed [redacted]	[redacted]	06/11/2024		
5.2	01/10/2025	Updated [redacted]	[redacted]	01/10/2025	[redacted]	

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

[redacted]

LIST OF EXHIBITS

LIST OF FIGURES

[redacted]

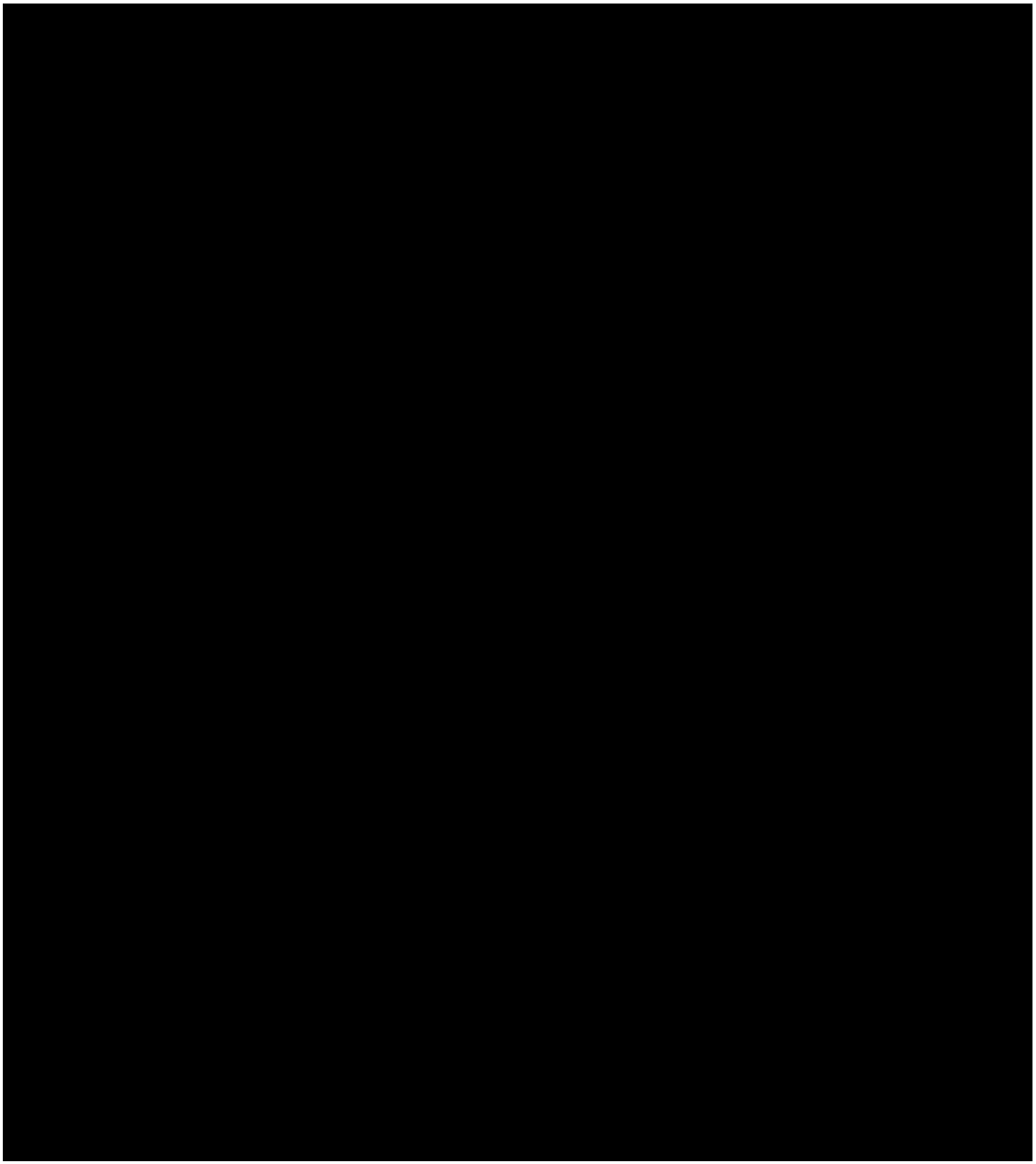
1. INTRODUCTION

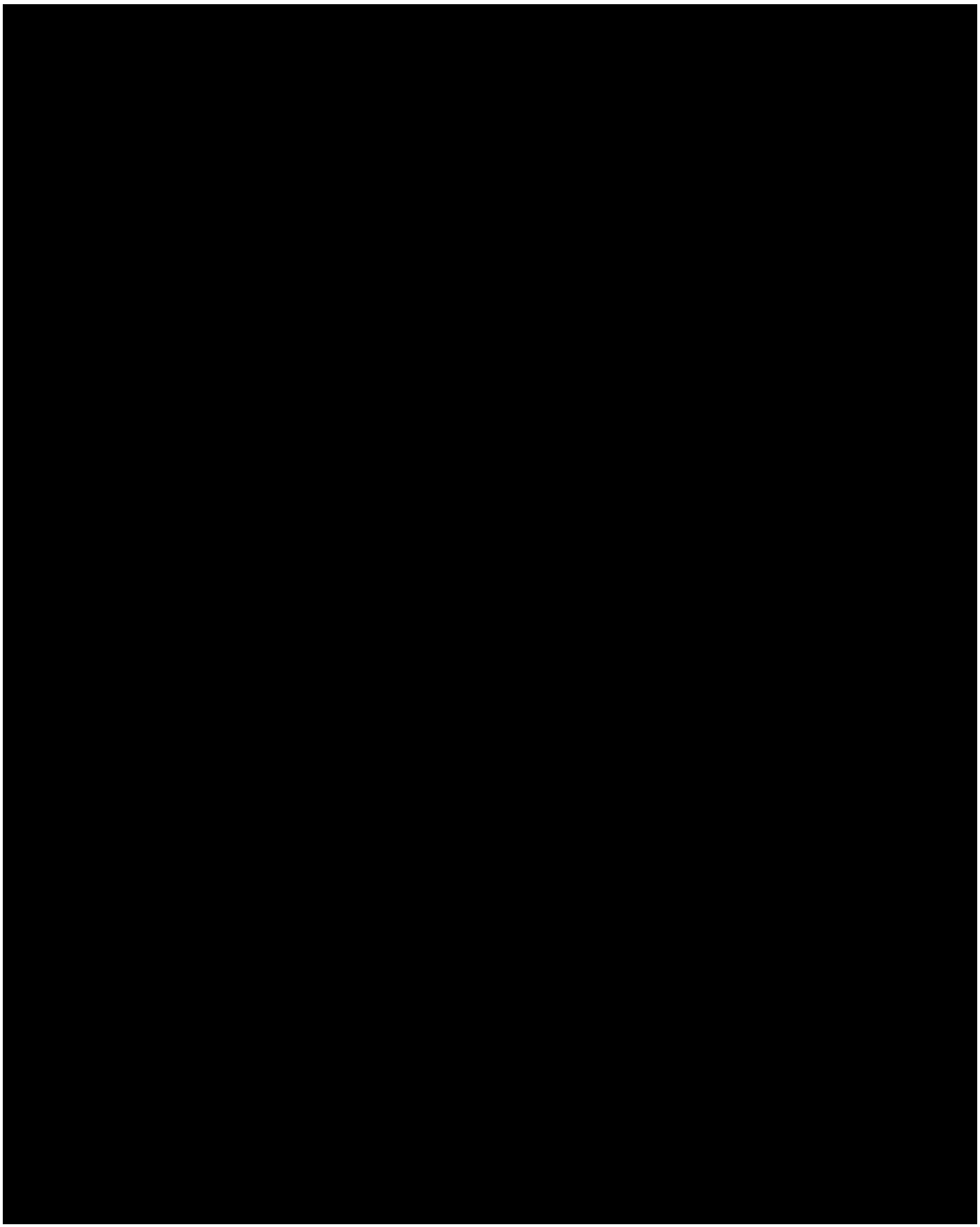
[redacted]

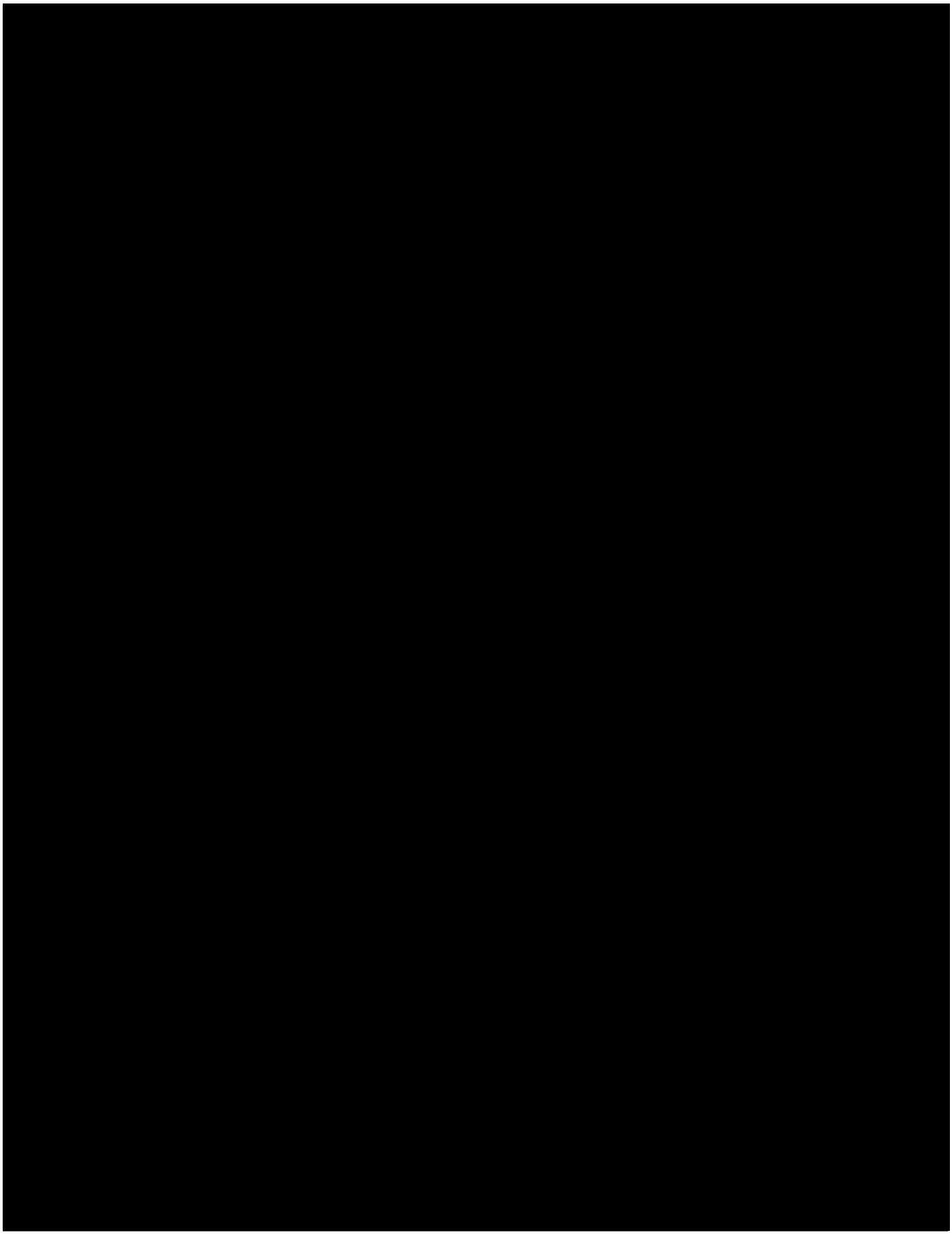
1.1 Overview

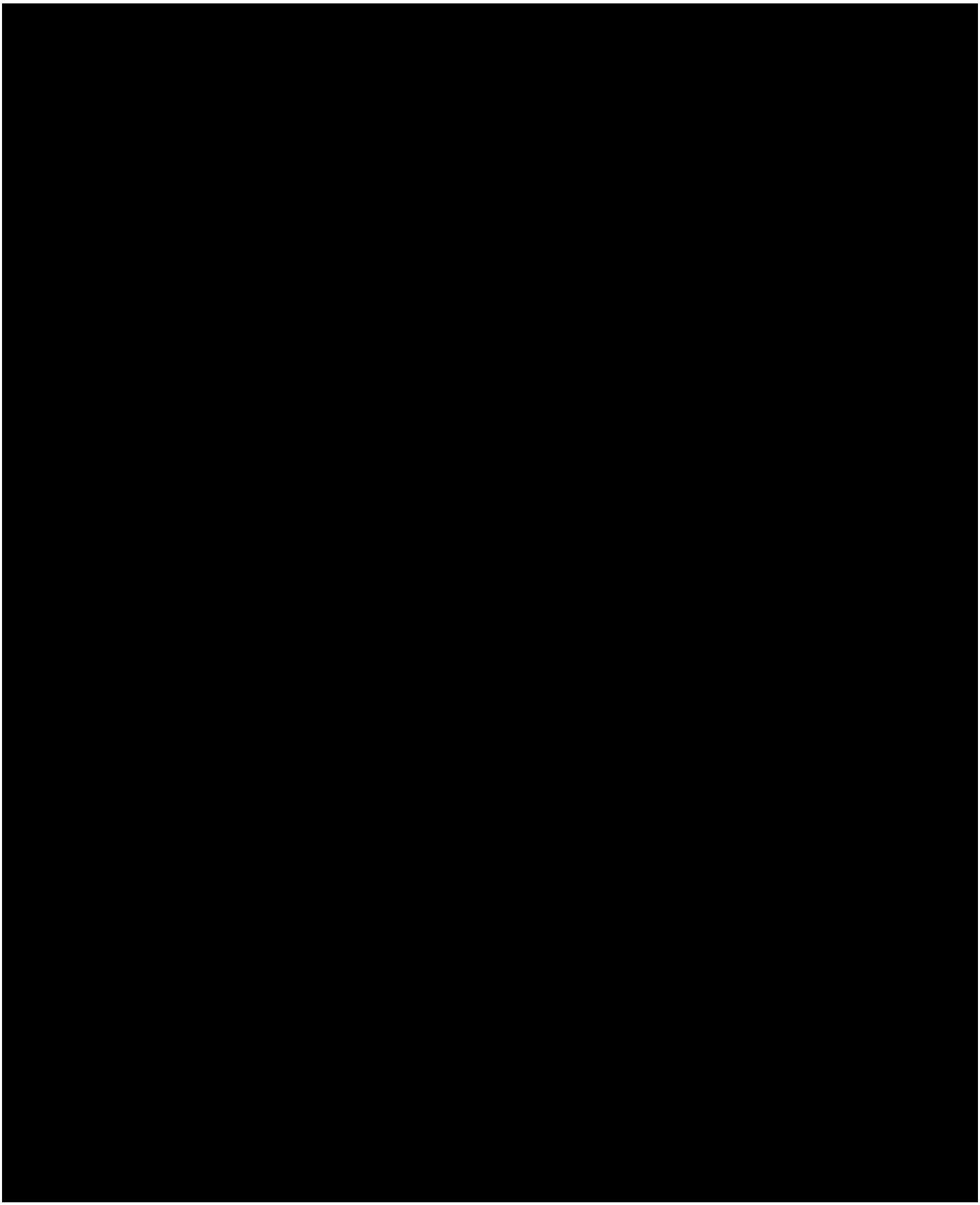
[redacted]

2. ISO ORIENTATION

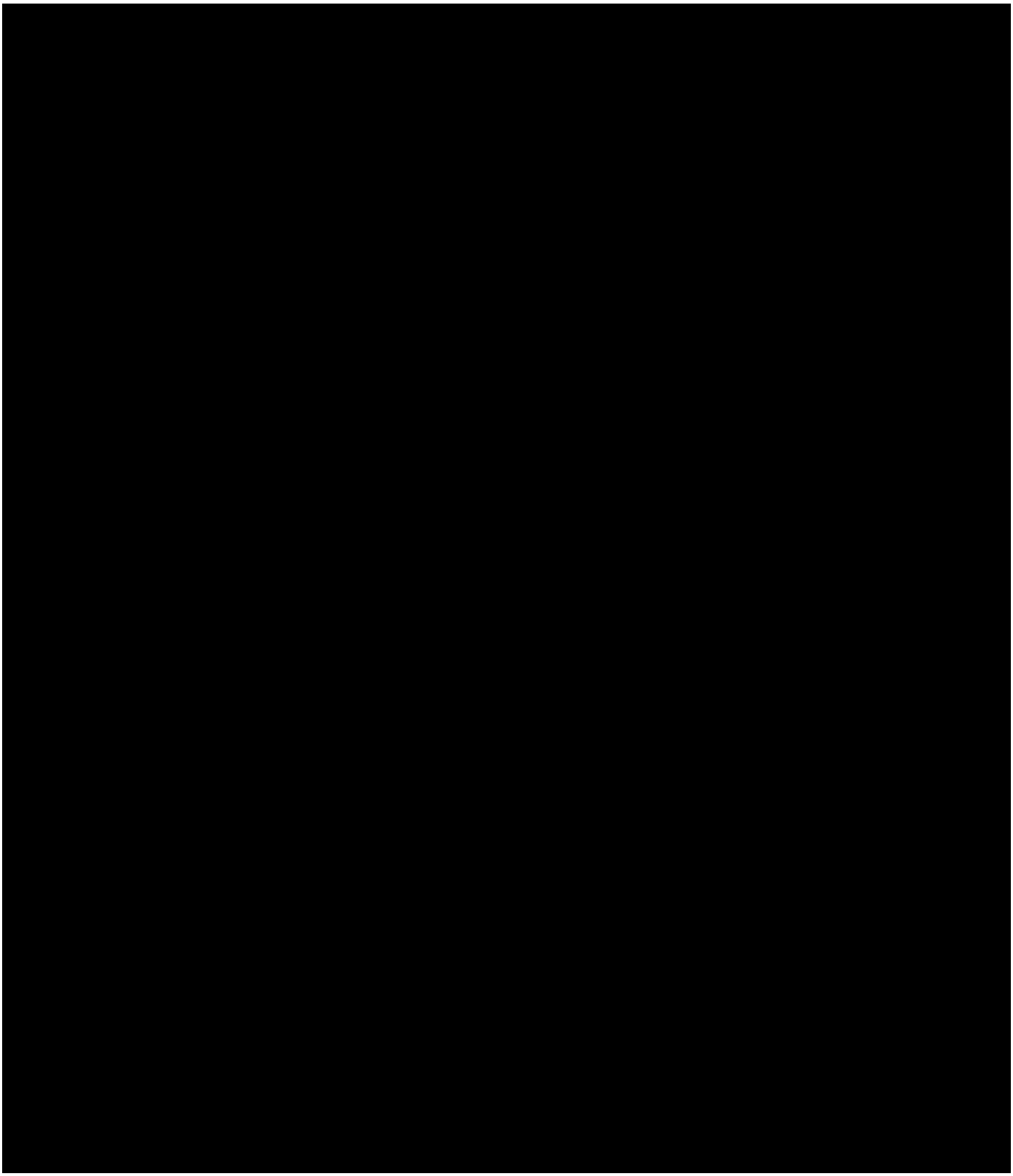


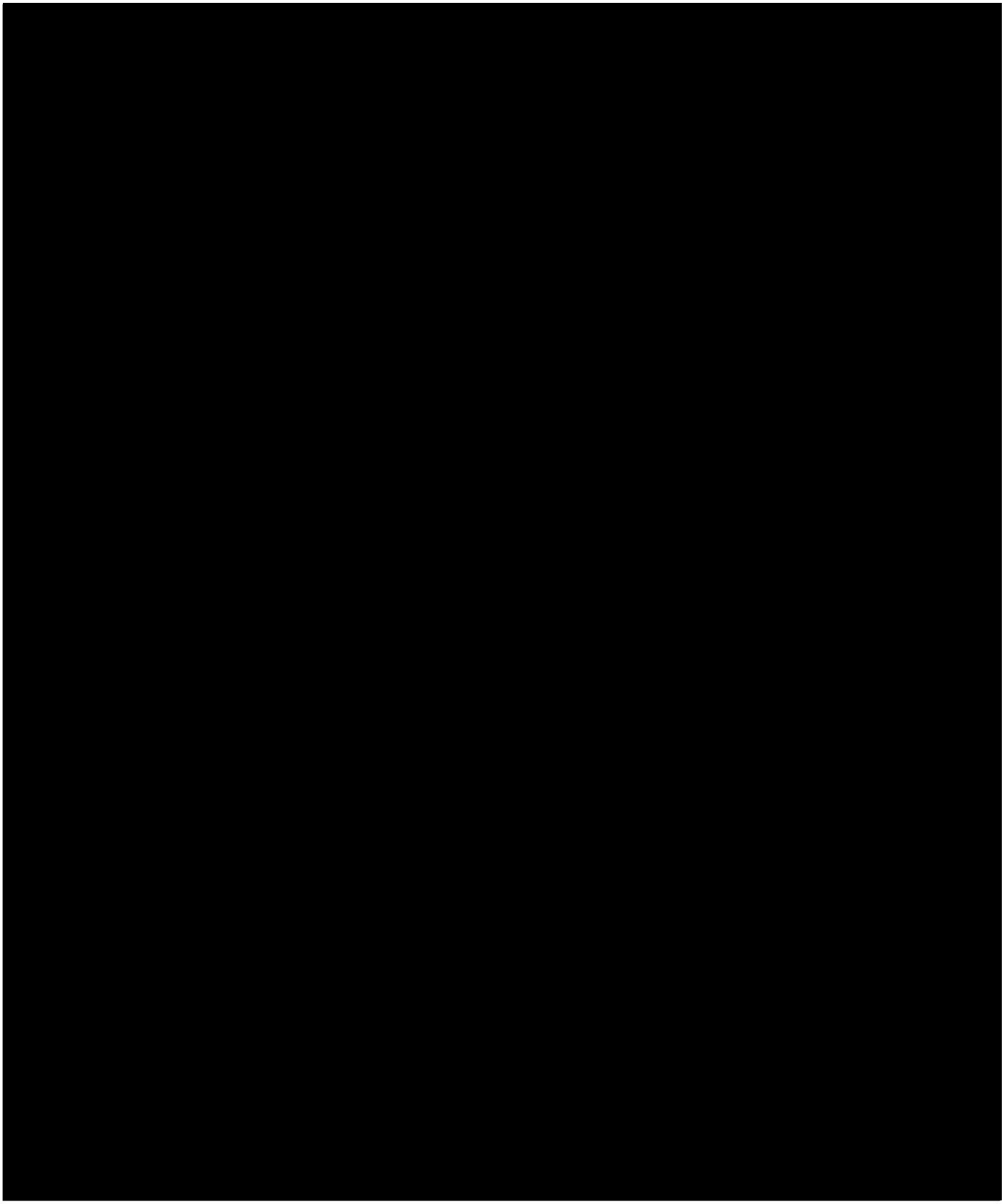


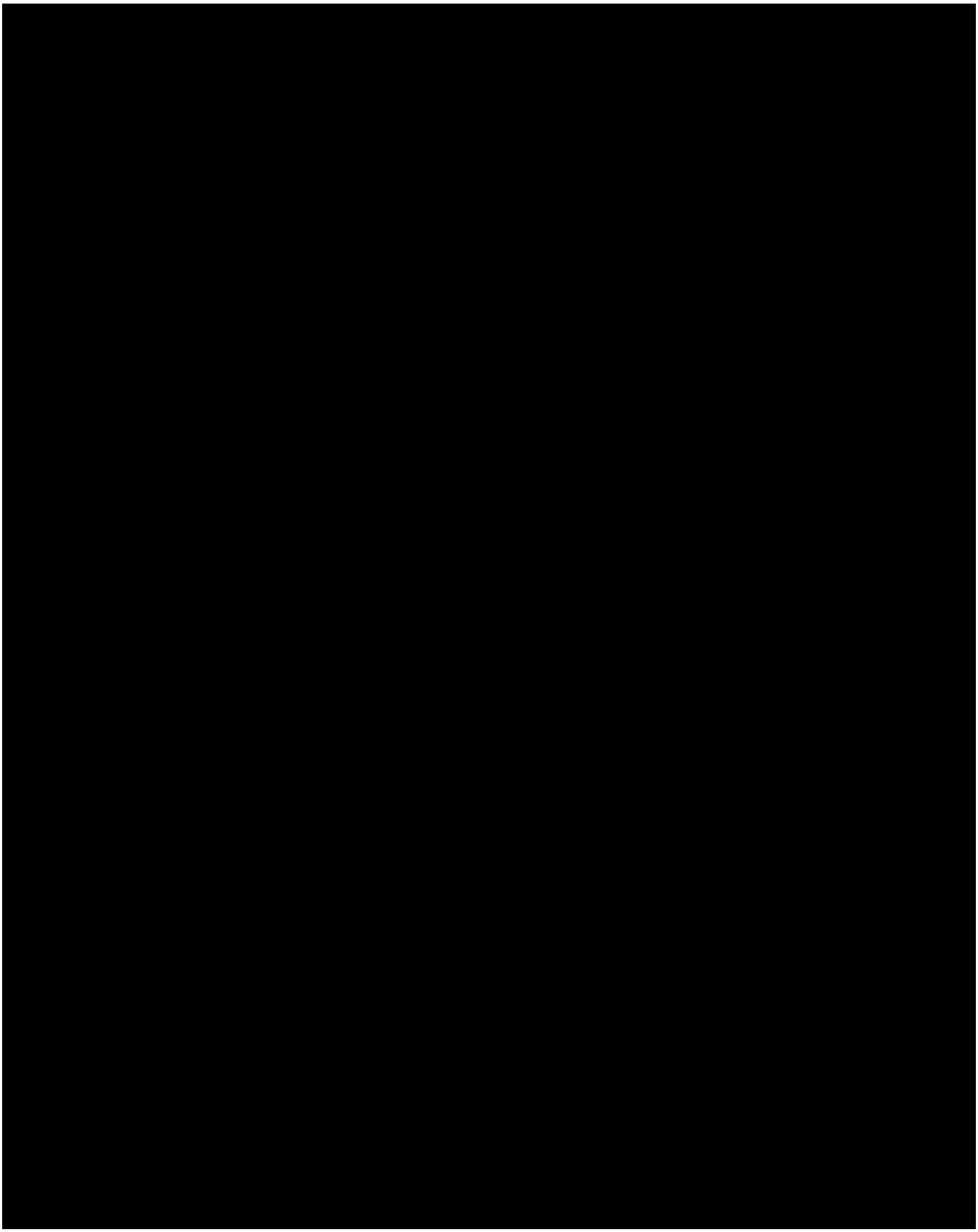


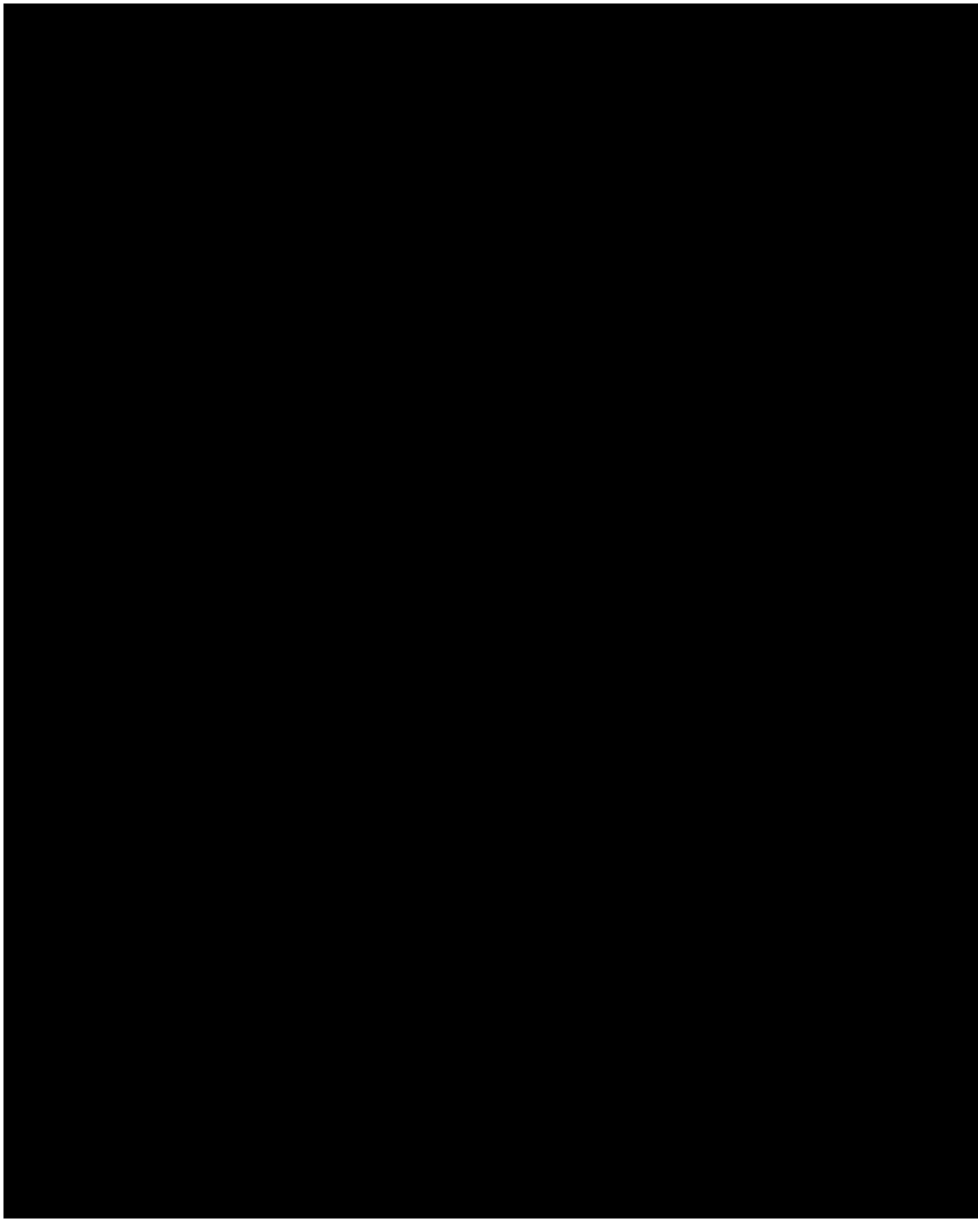


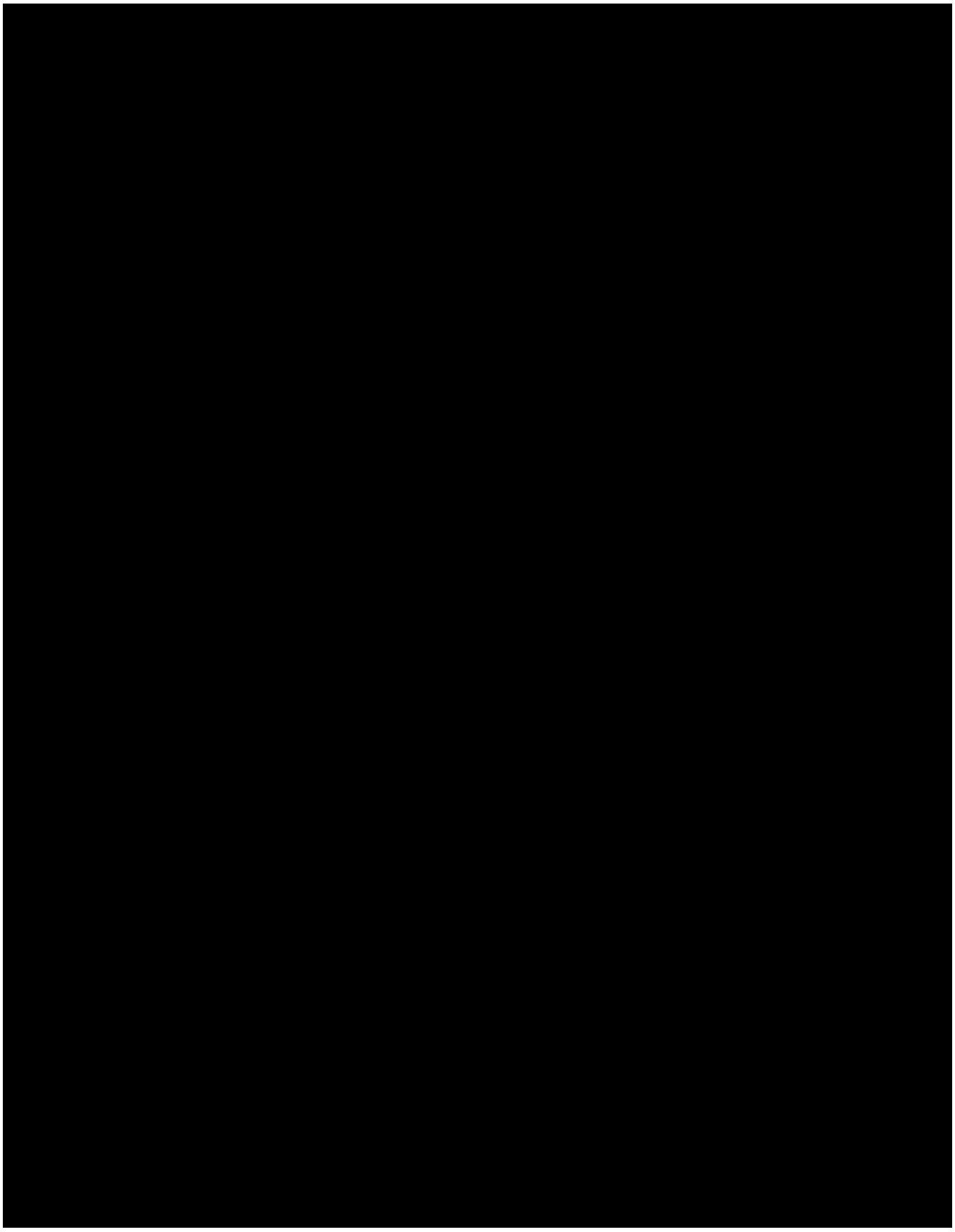
3. ACCESS CONTROL ADMINISRATION

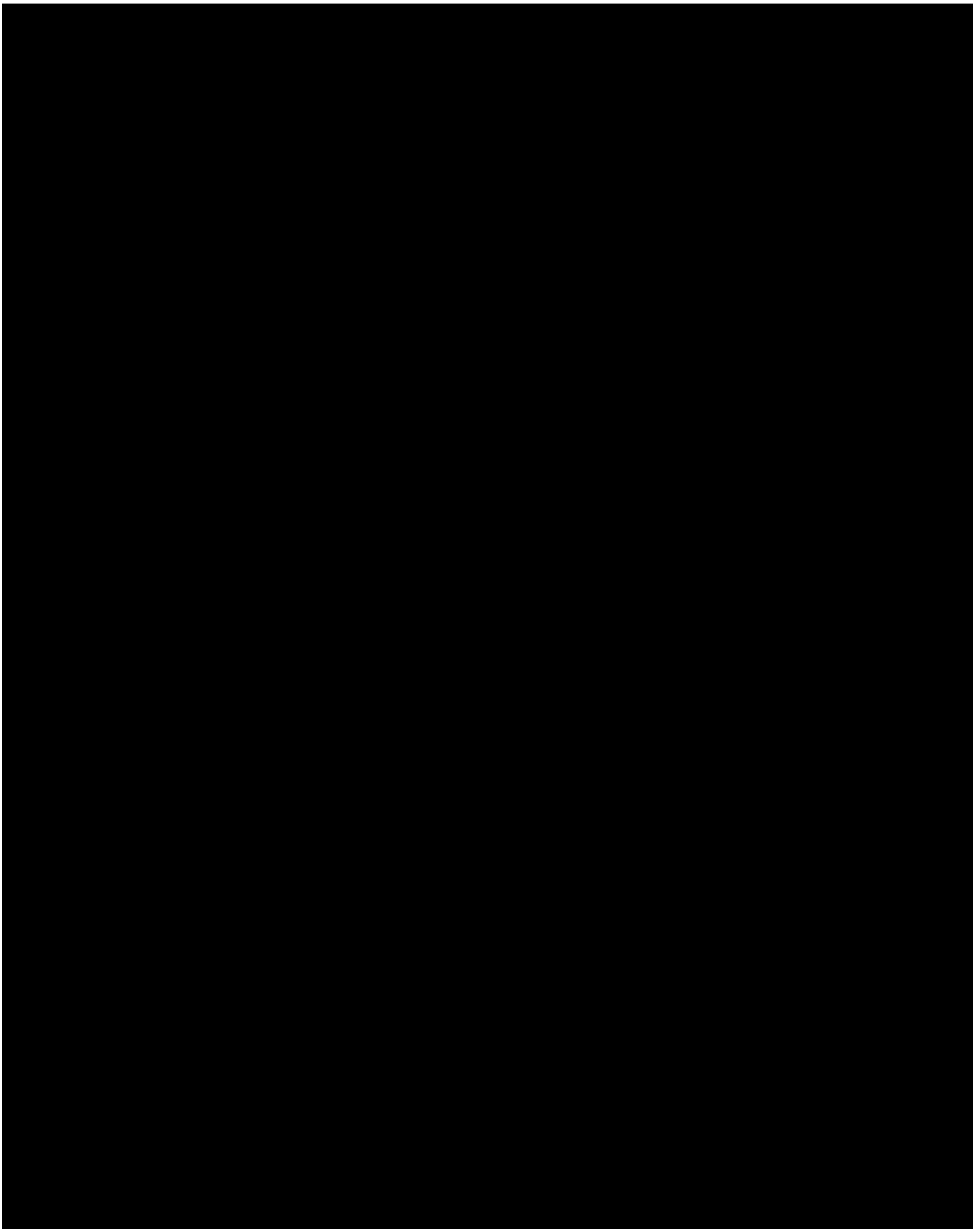


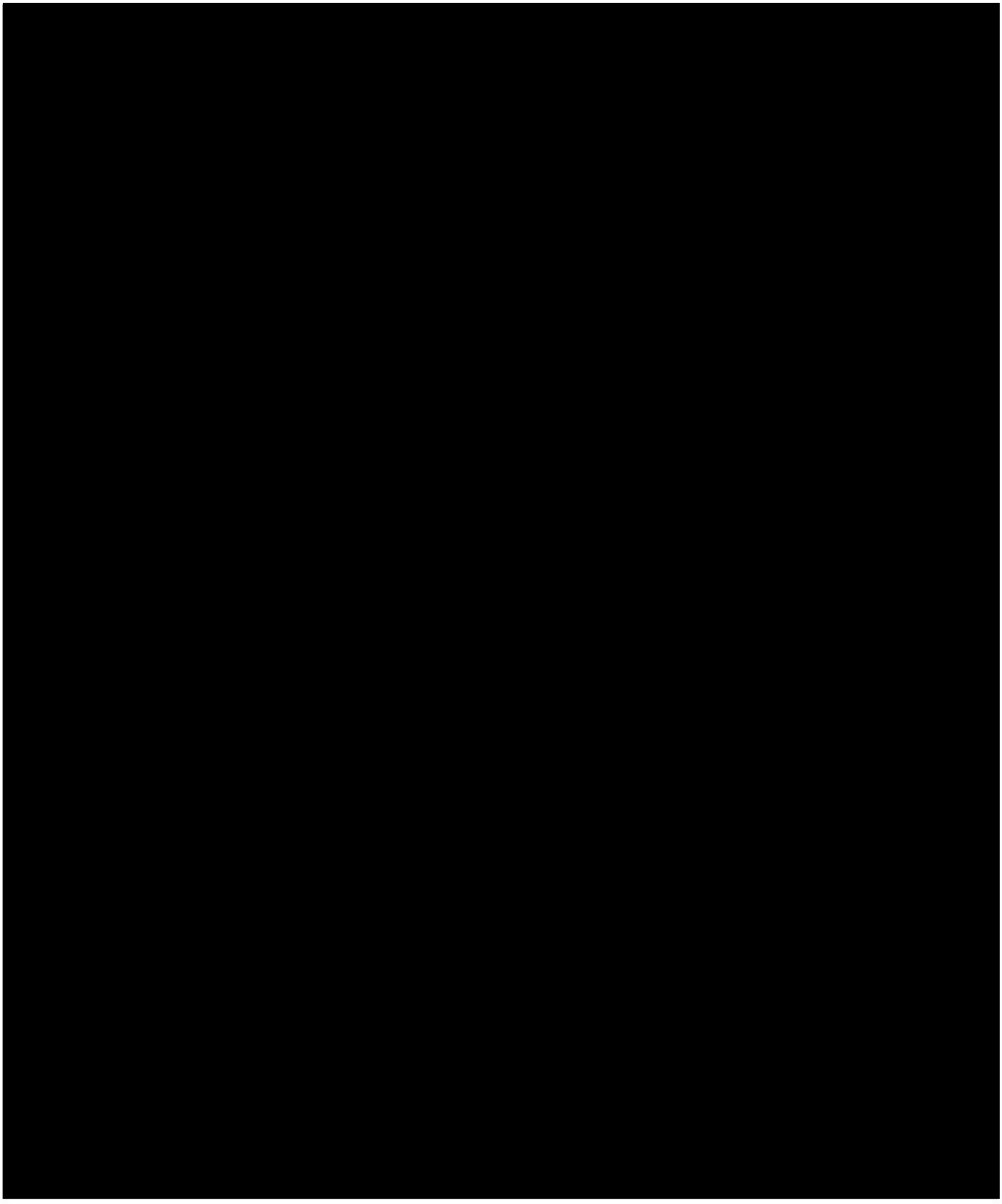


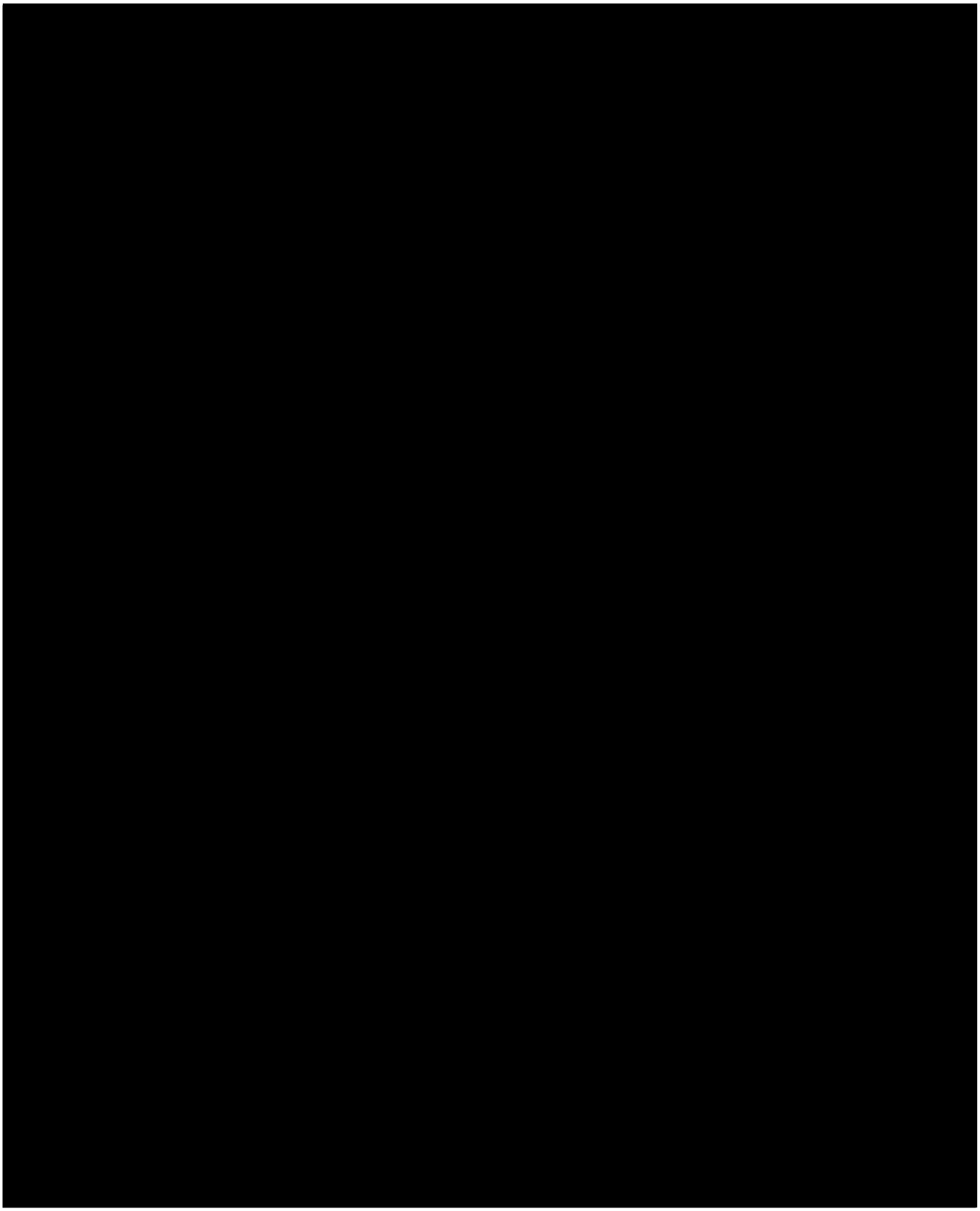


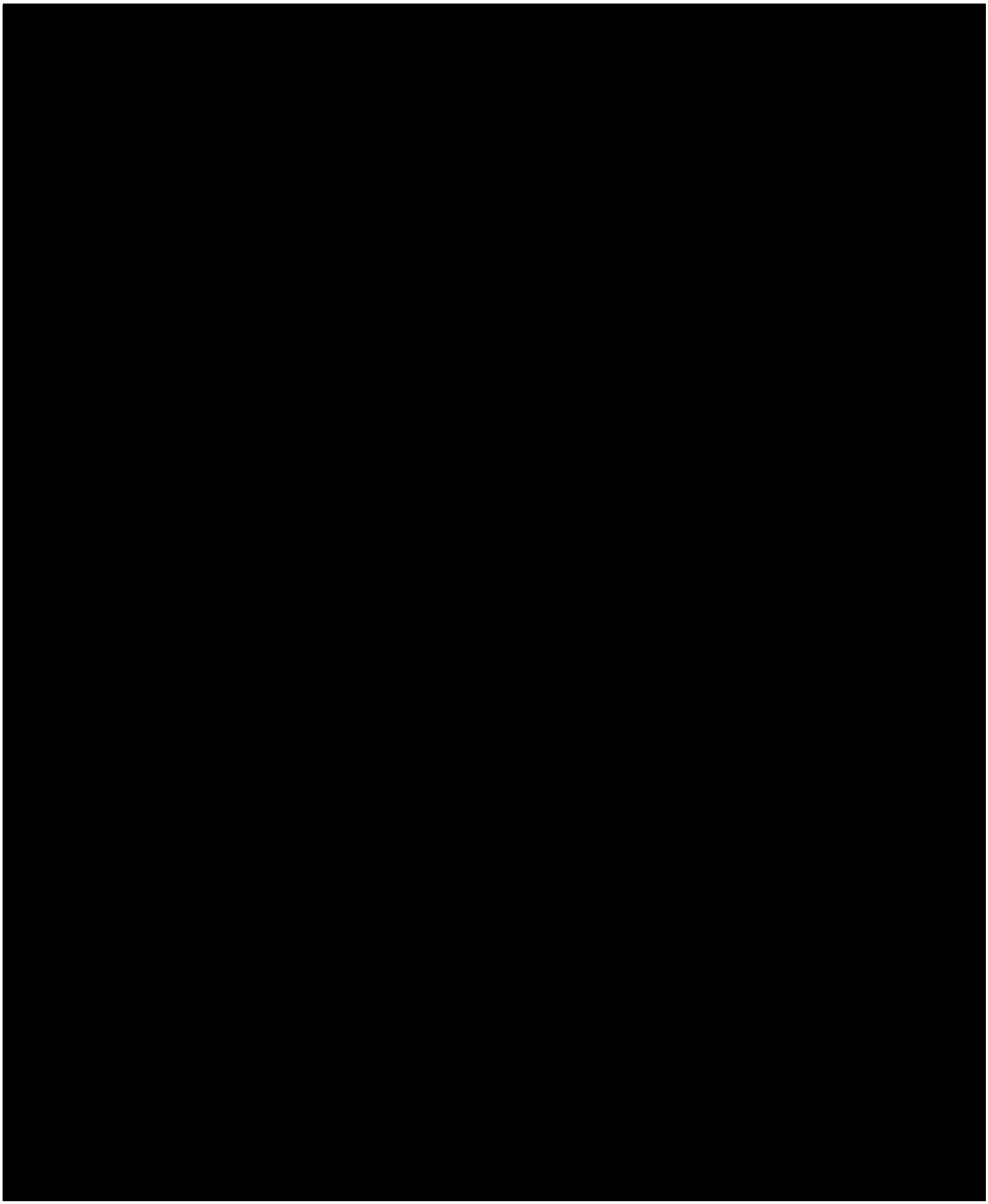


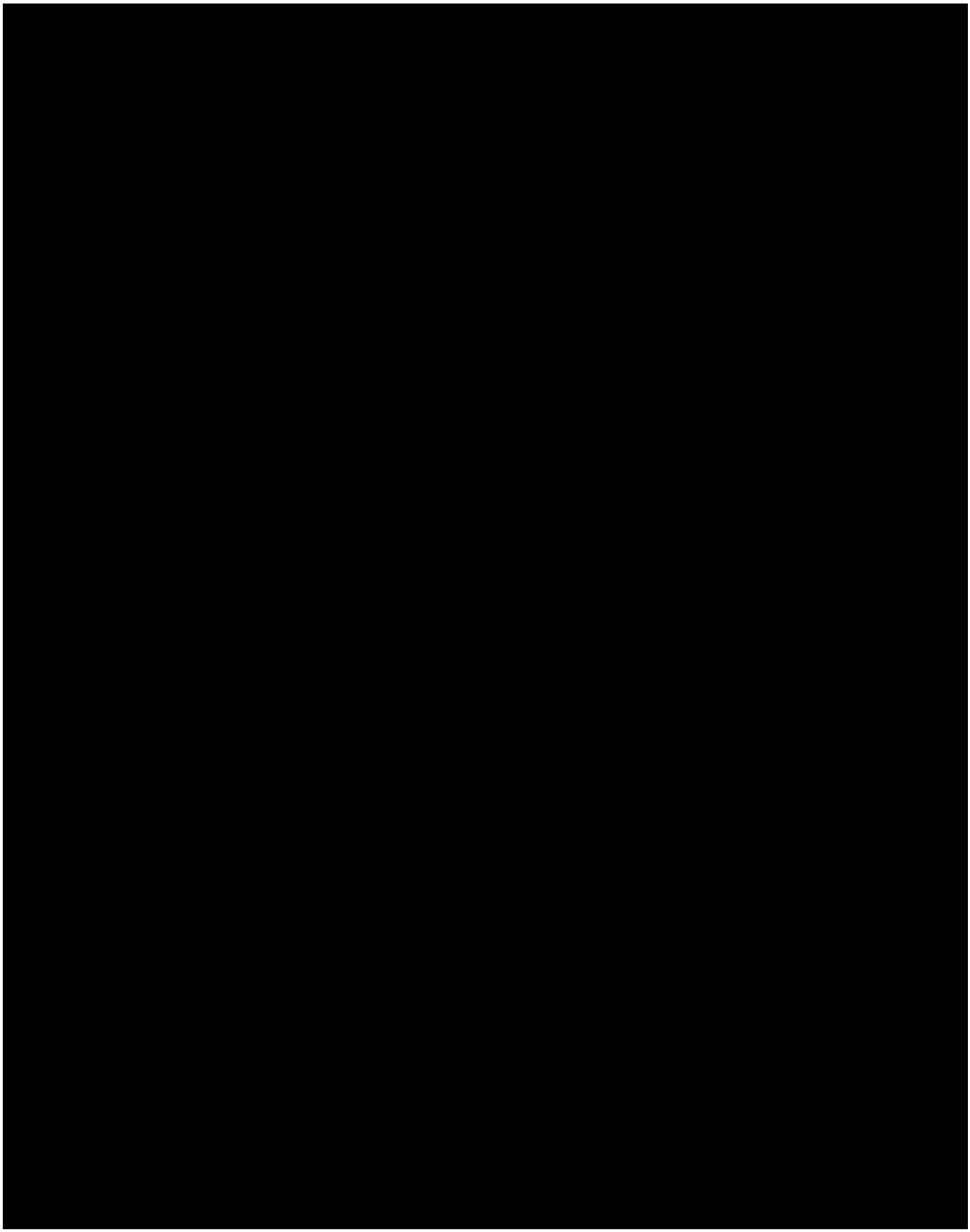


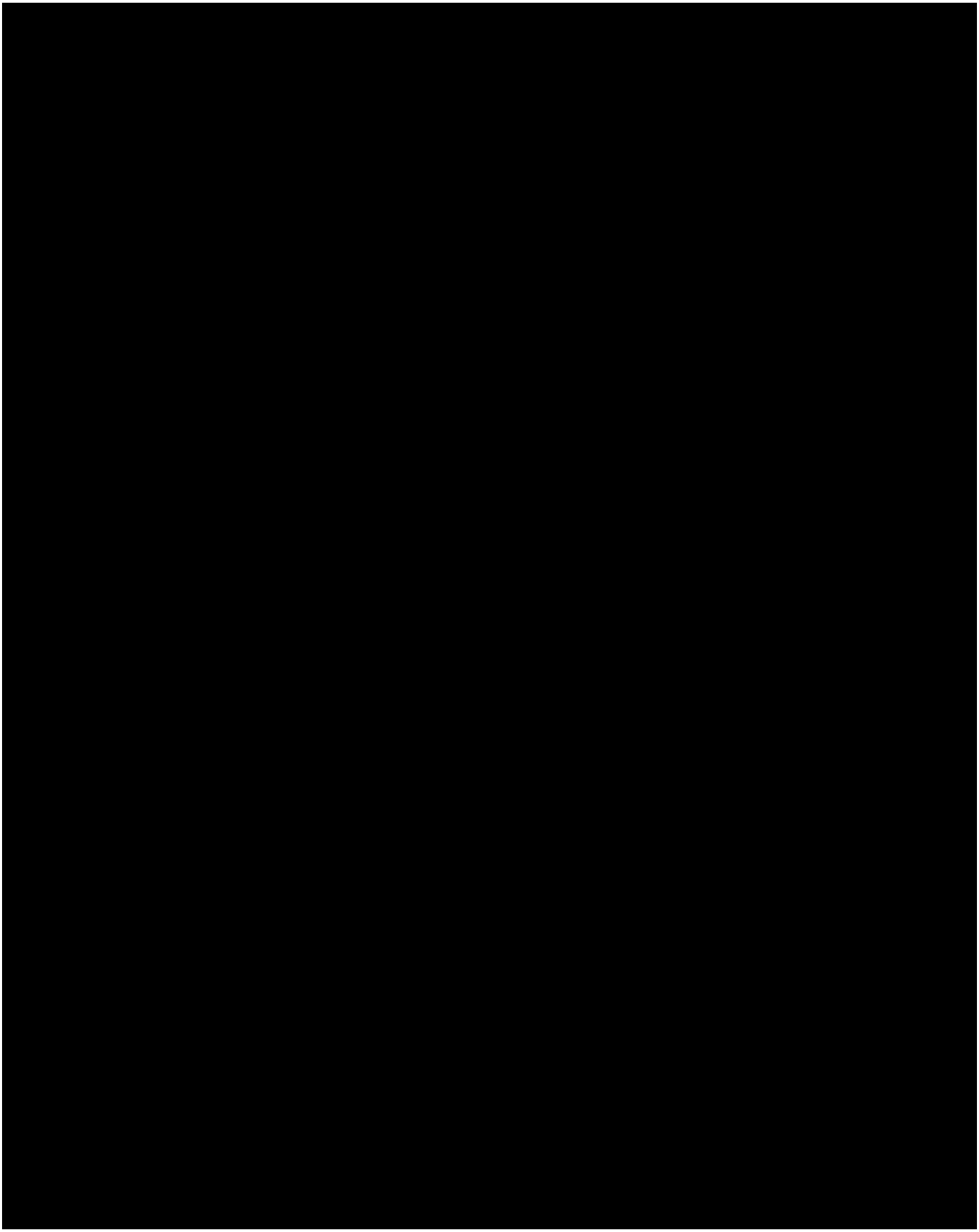


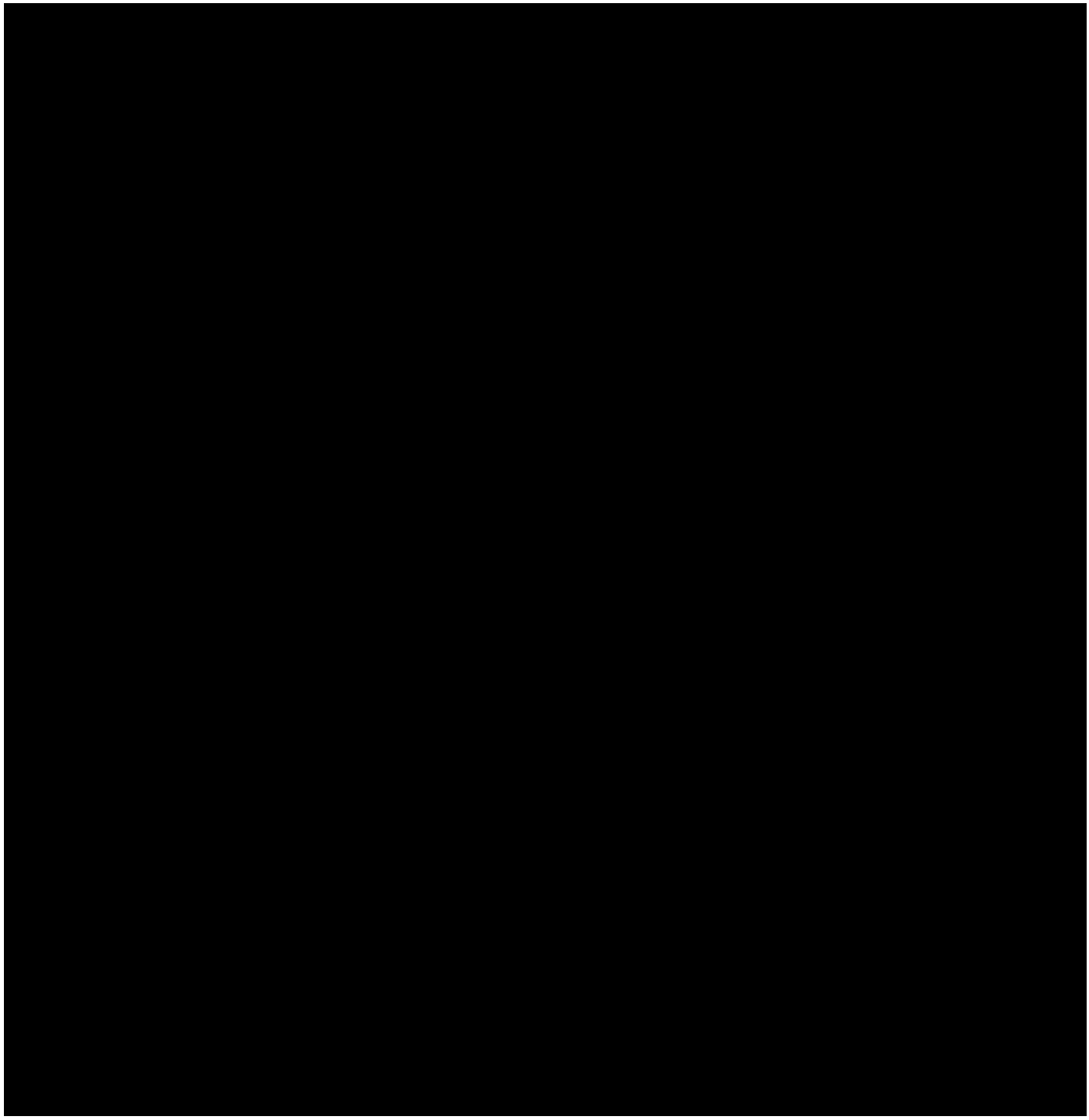


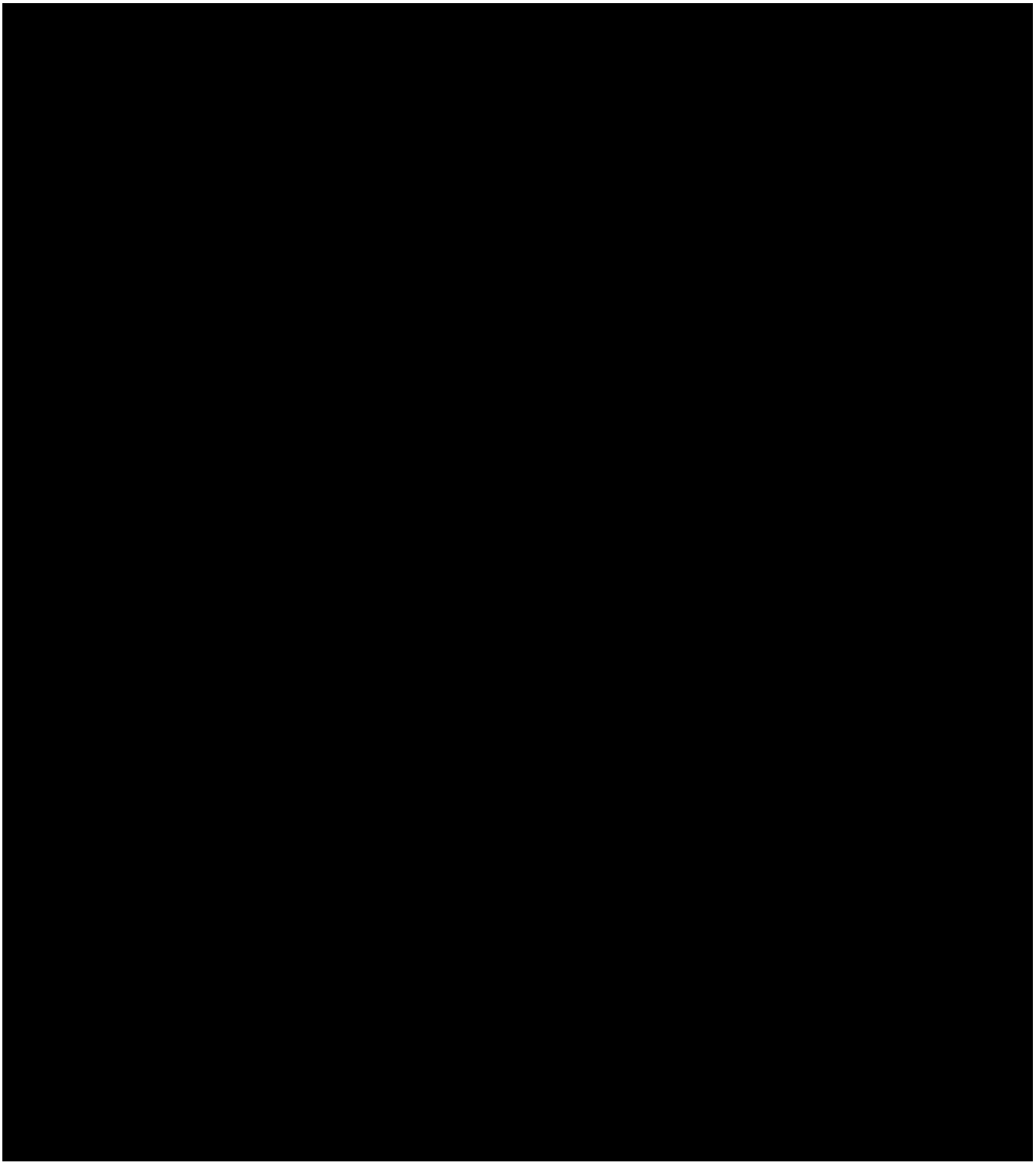


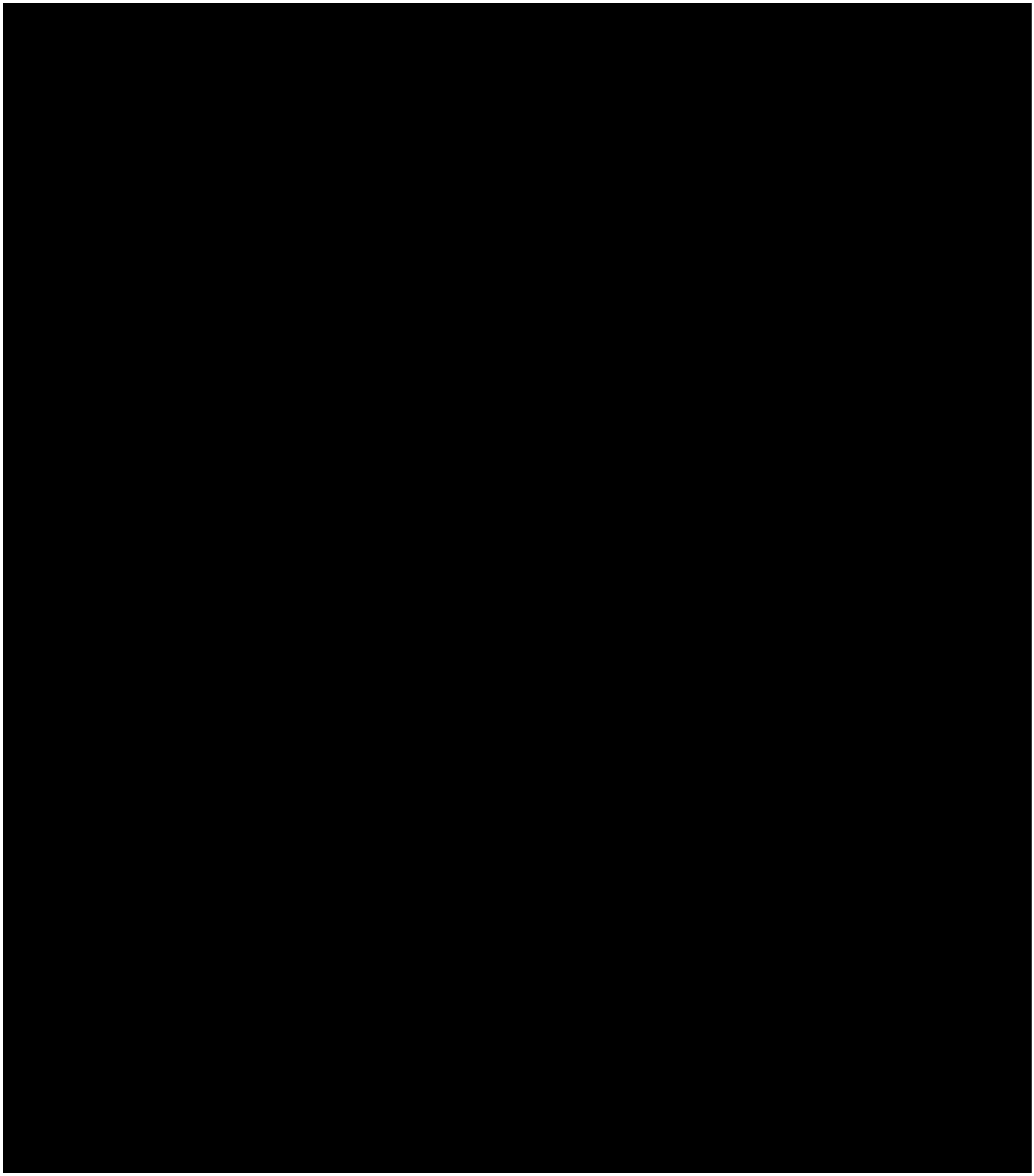


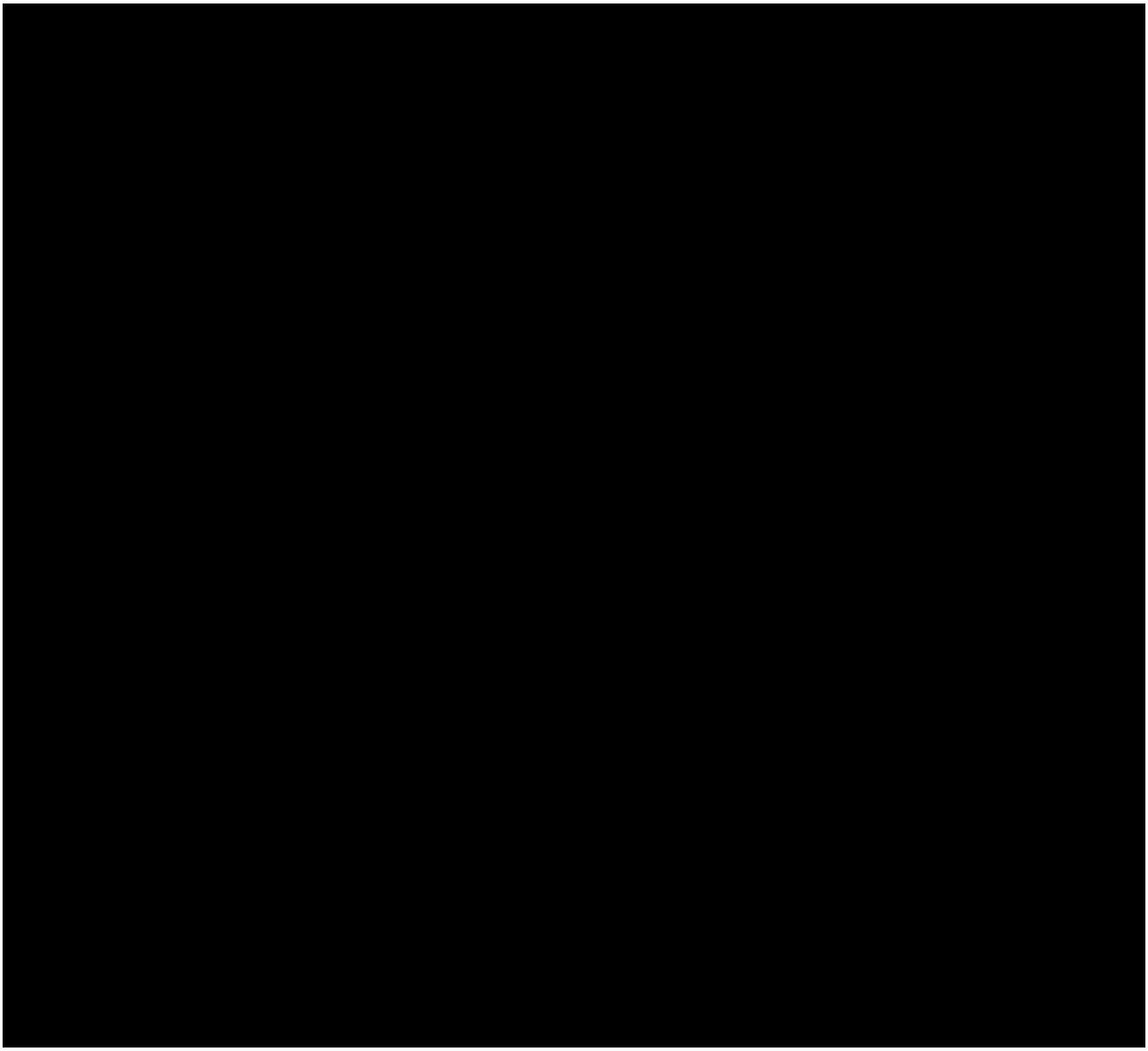


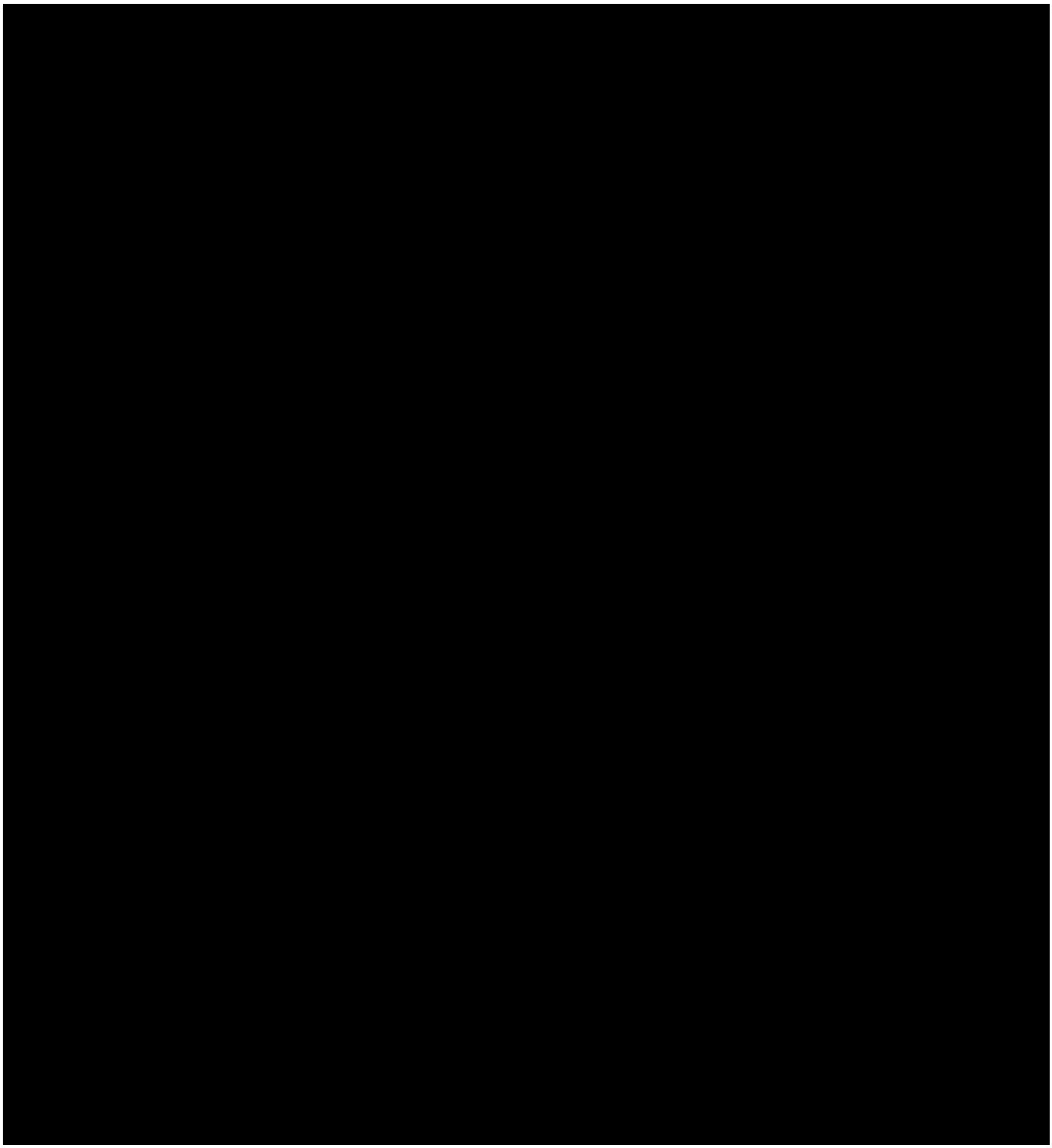


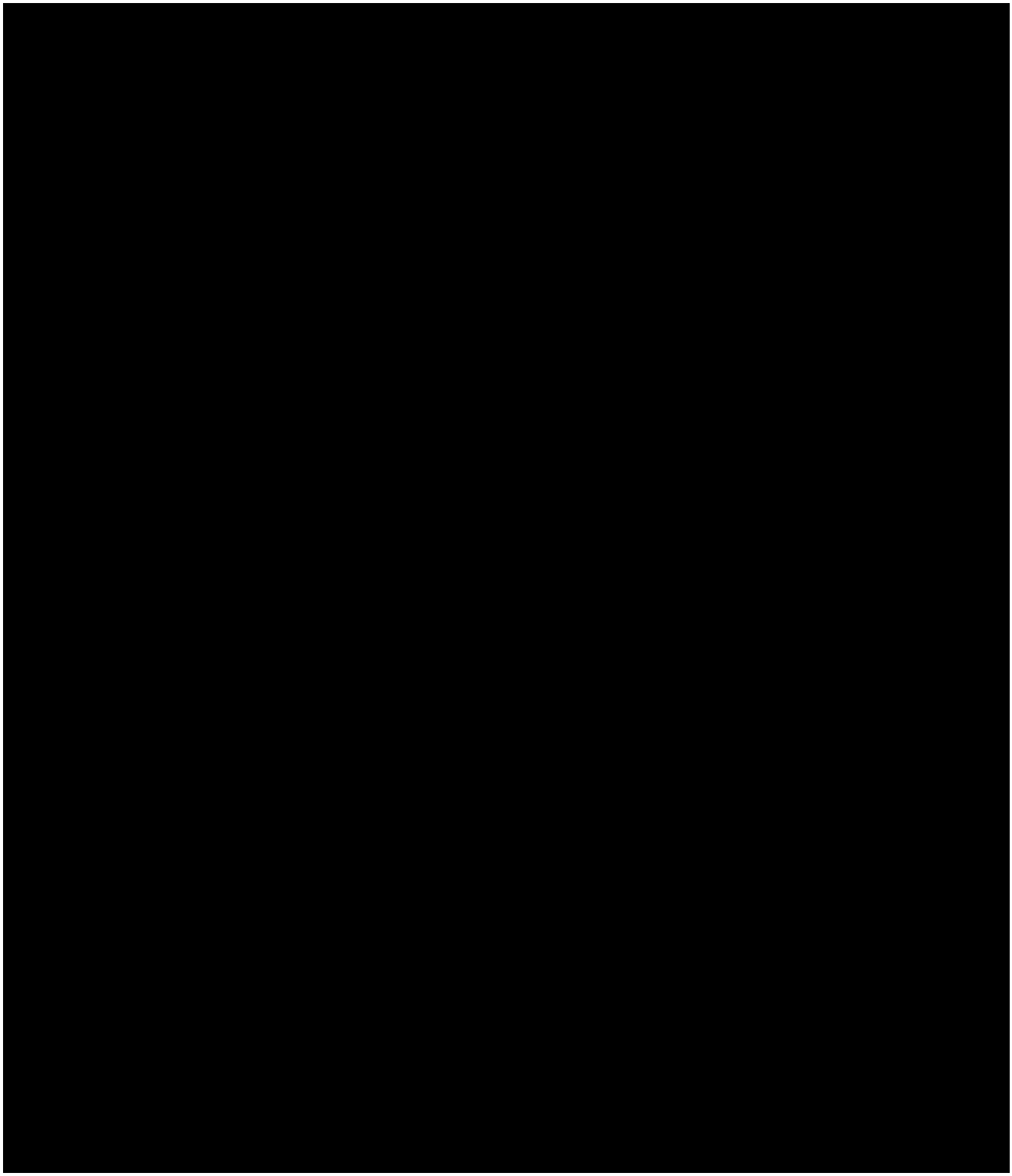


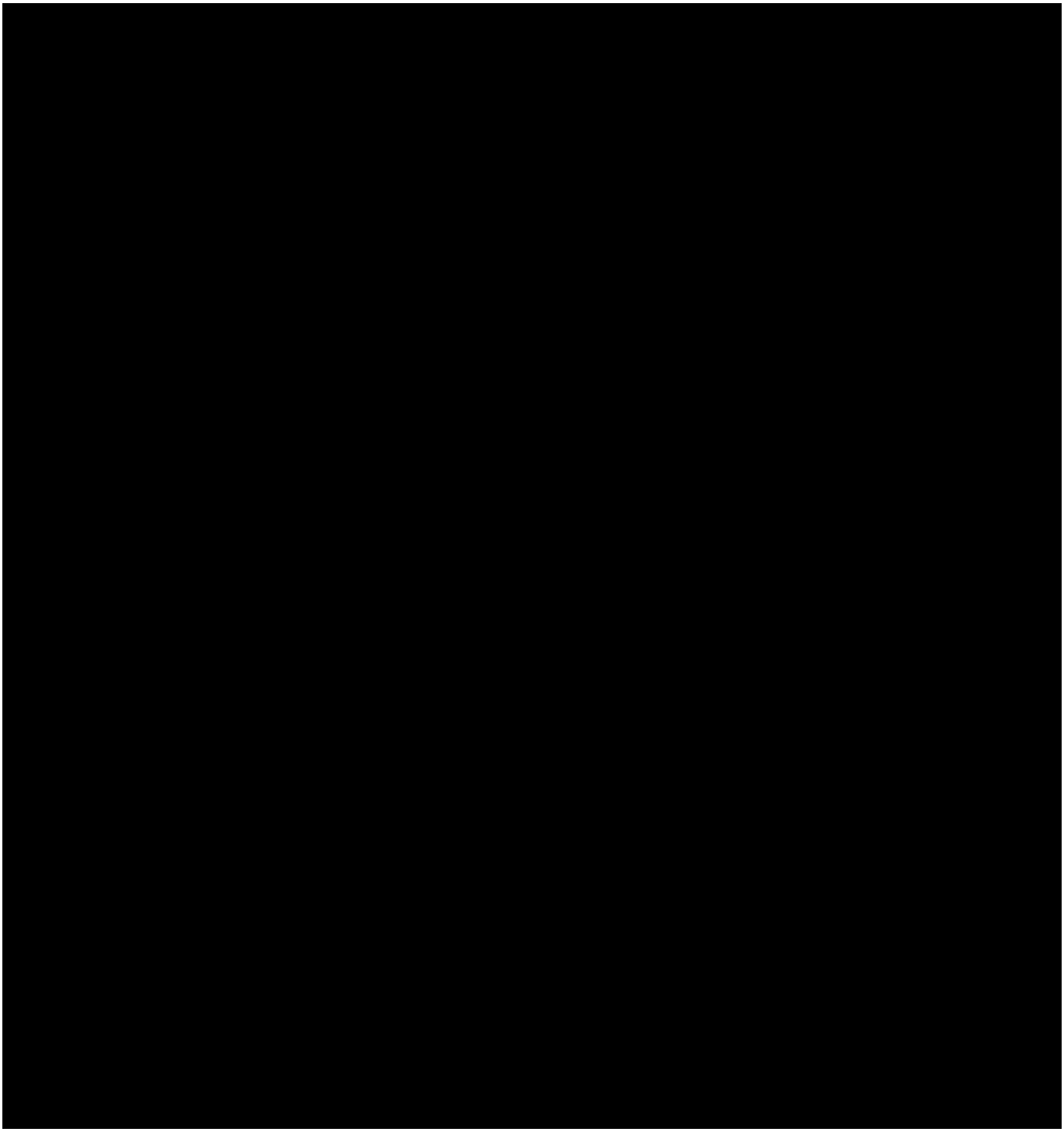


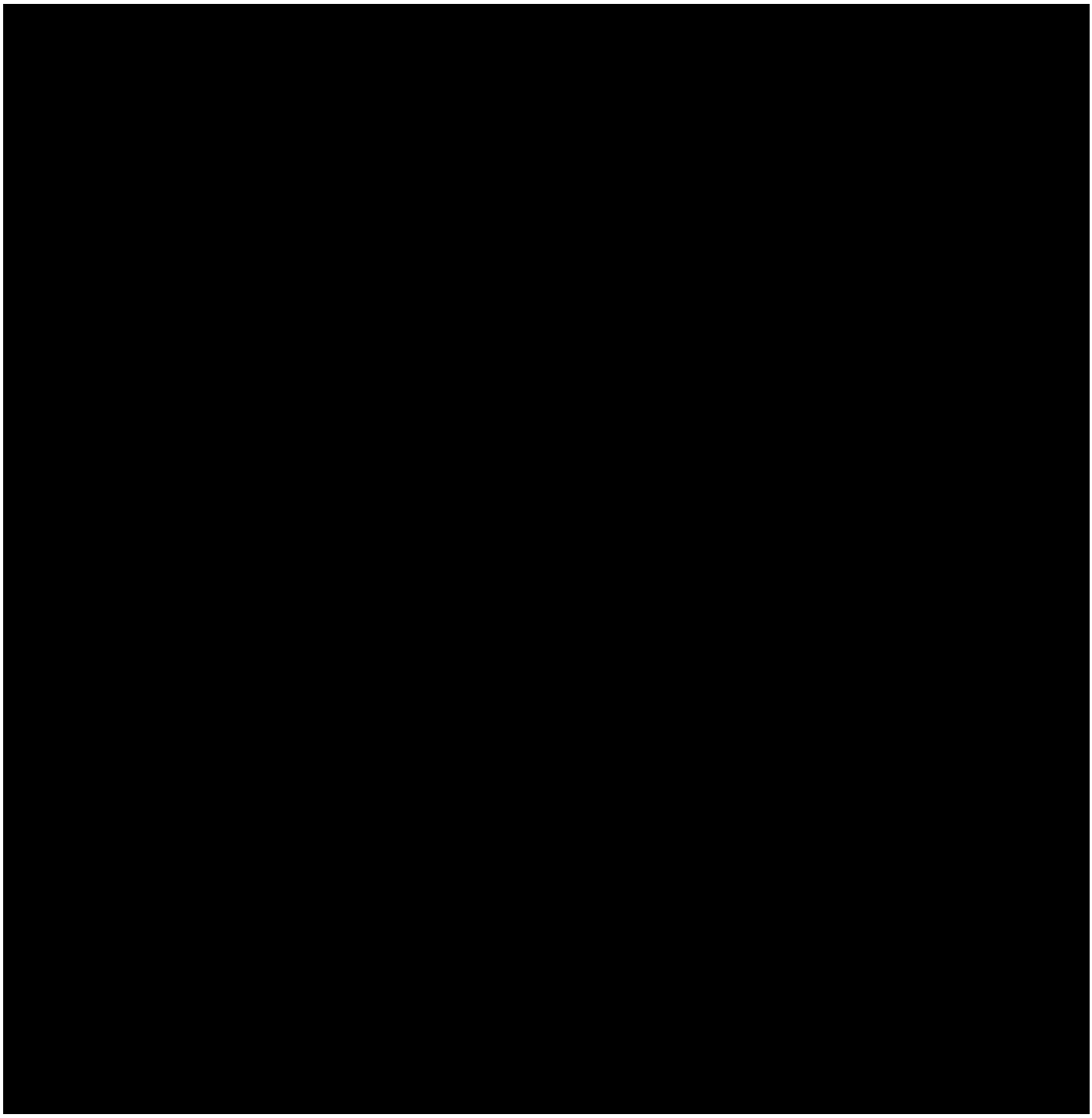


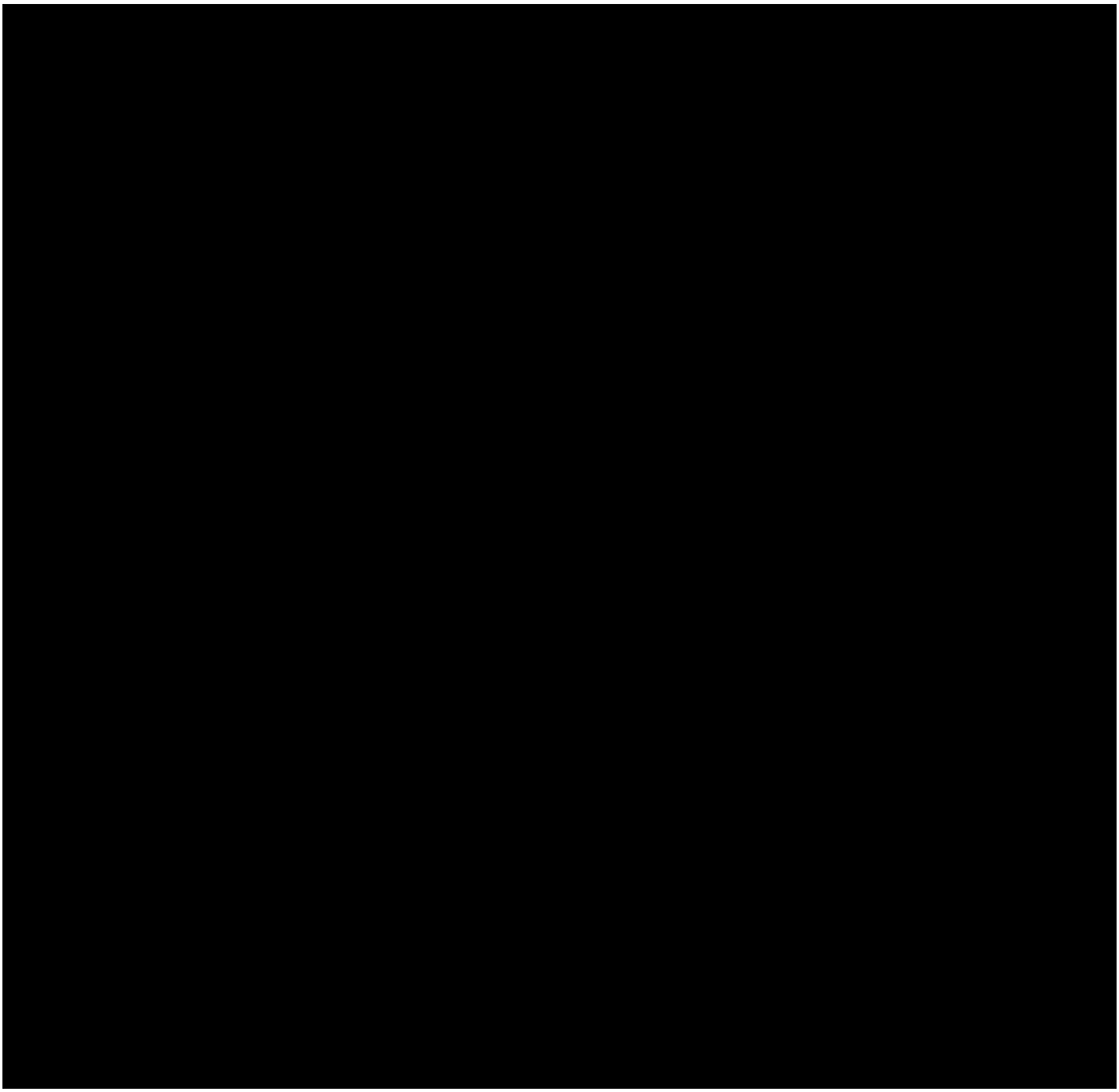


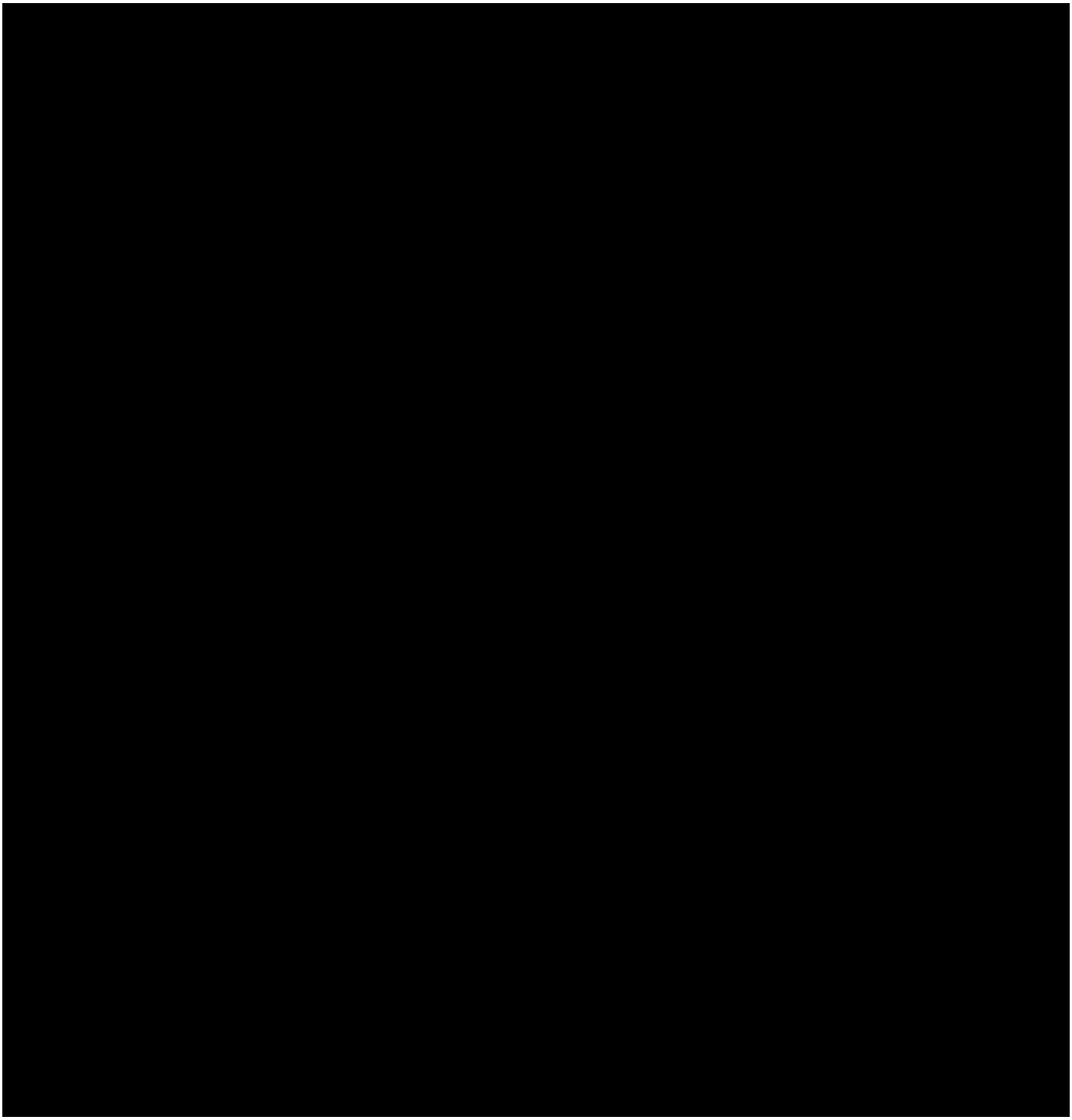


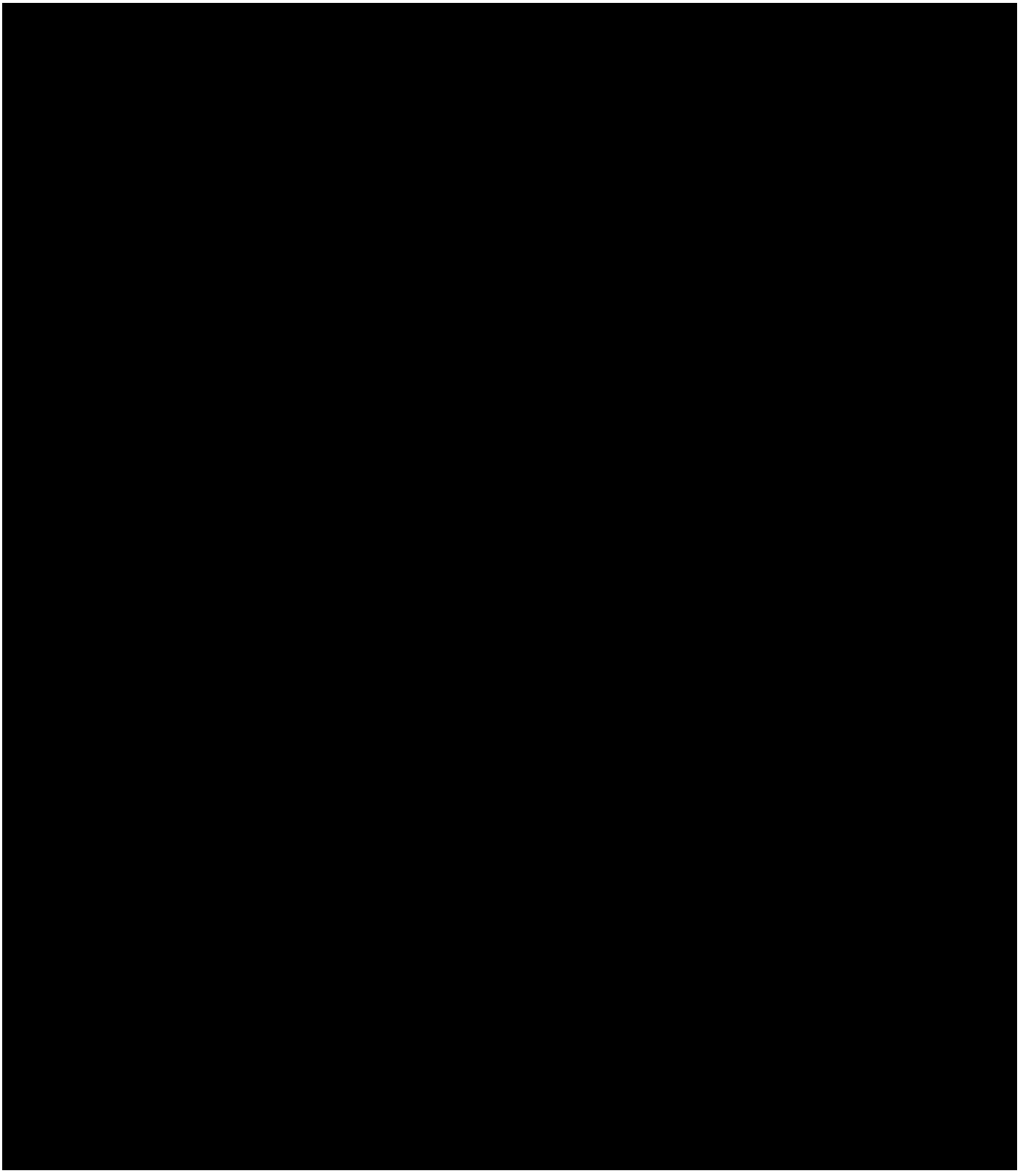


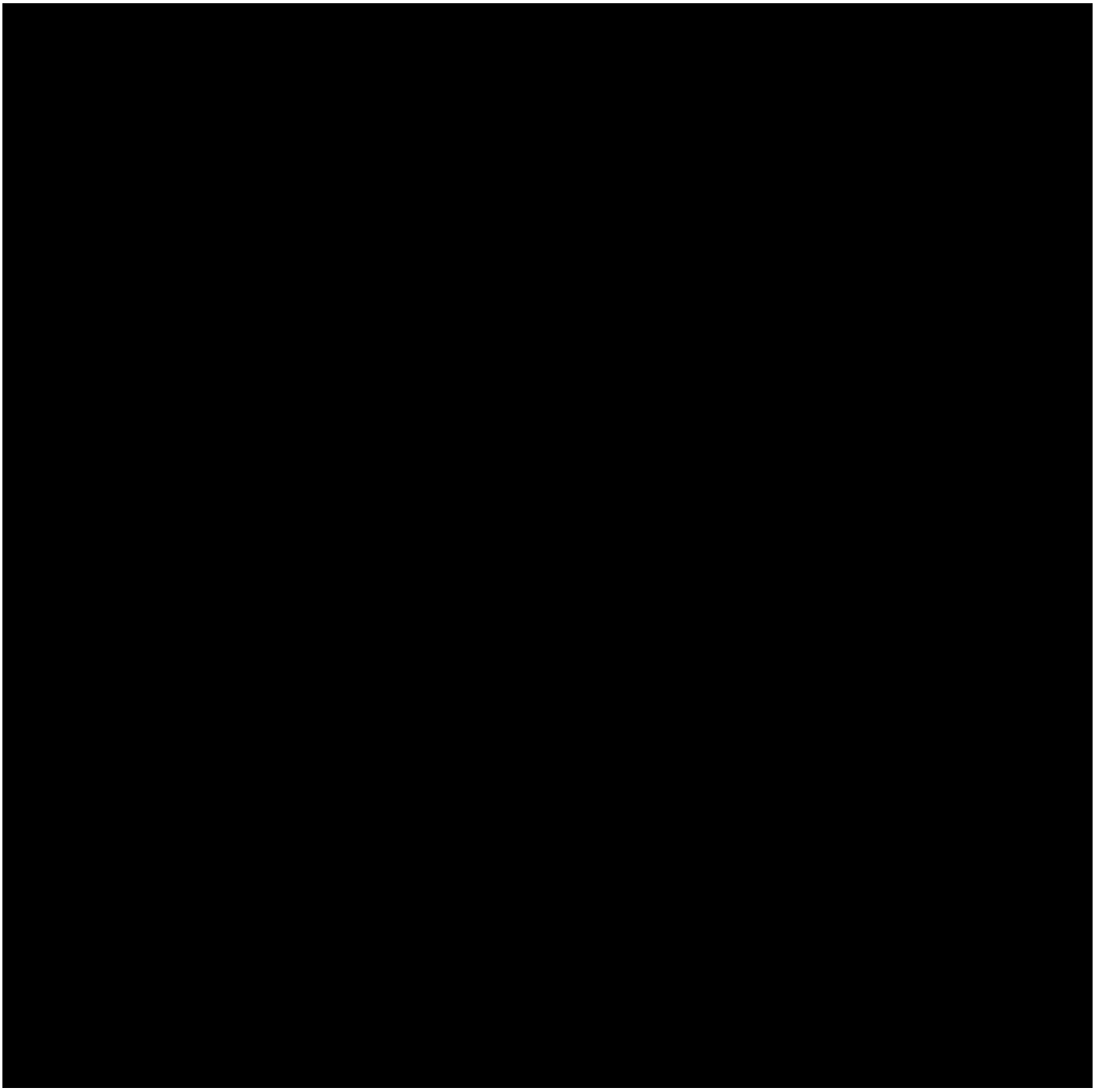


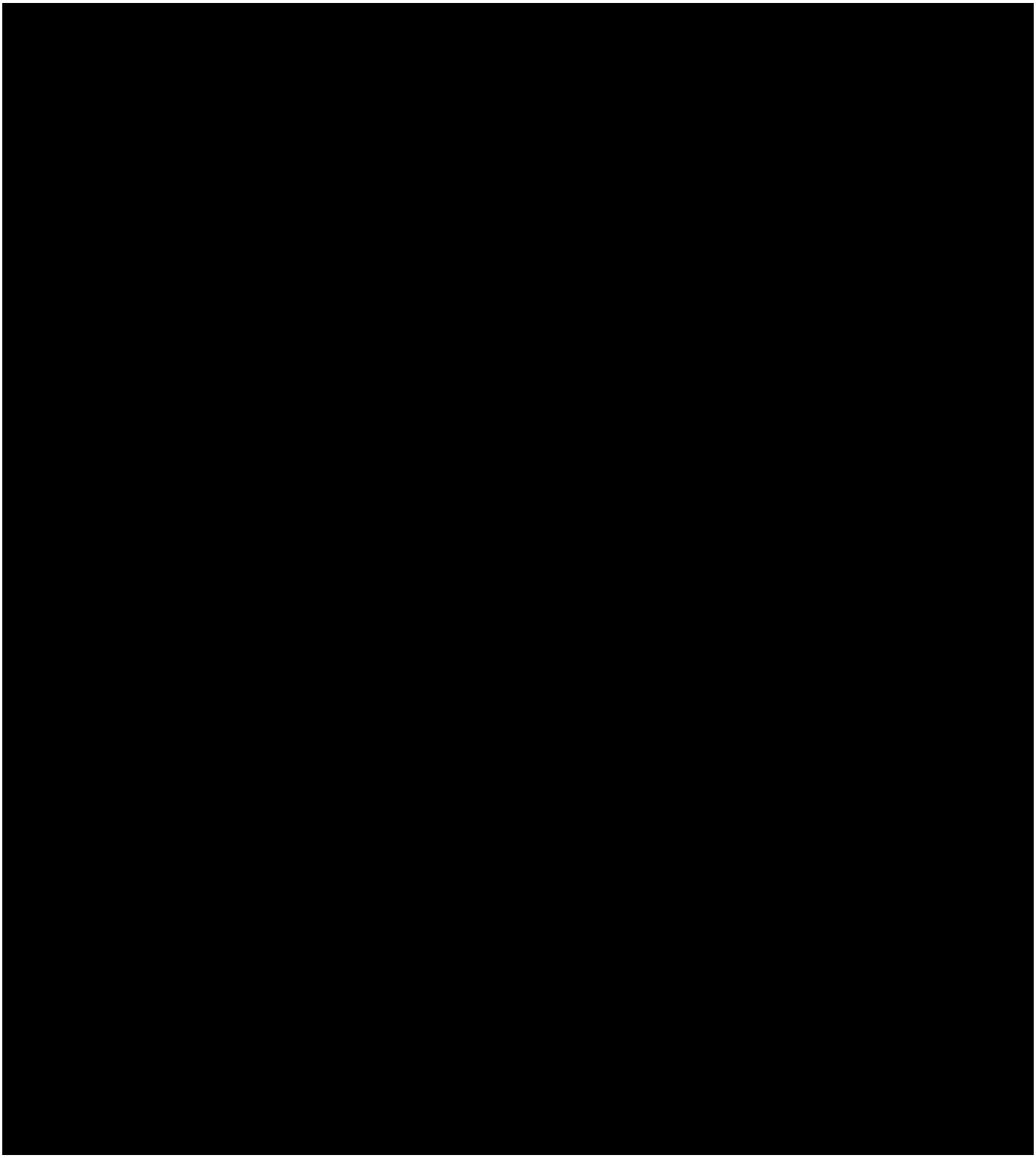


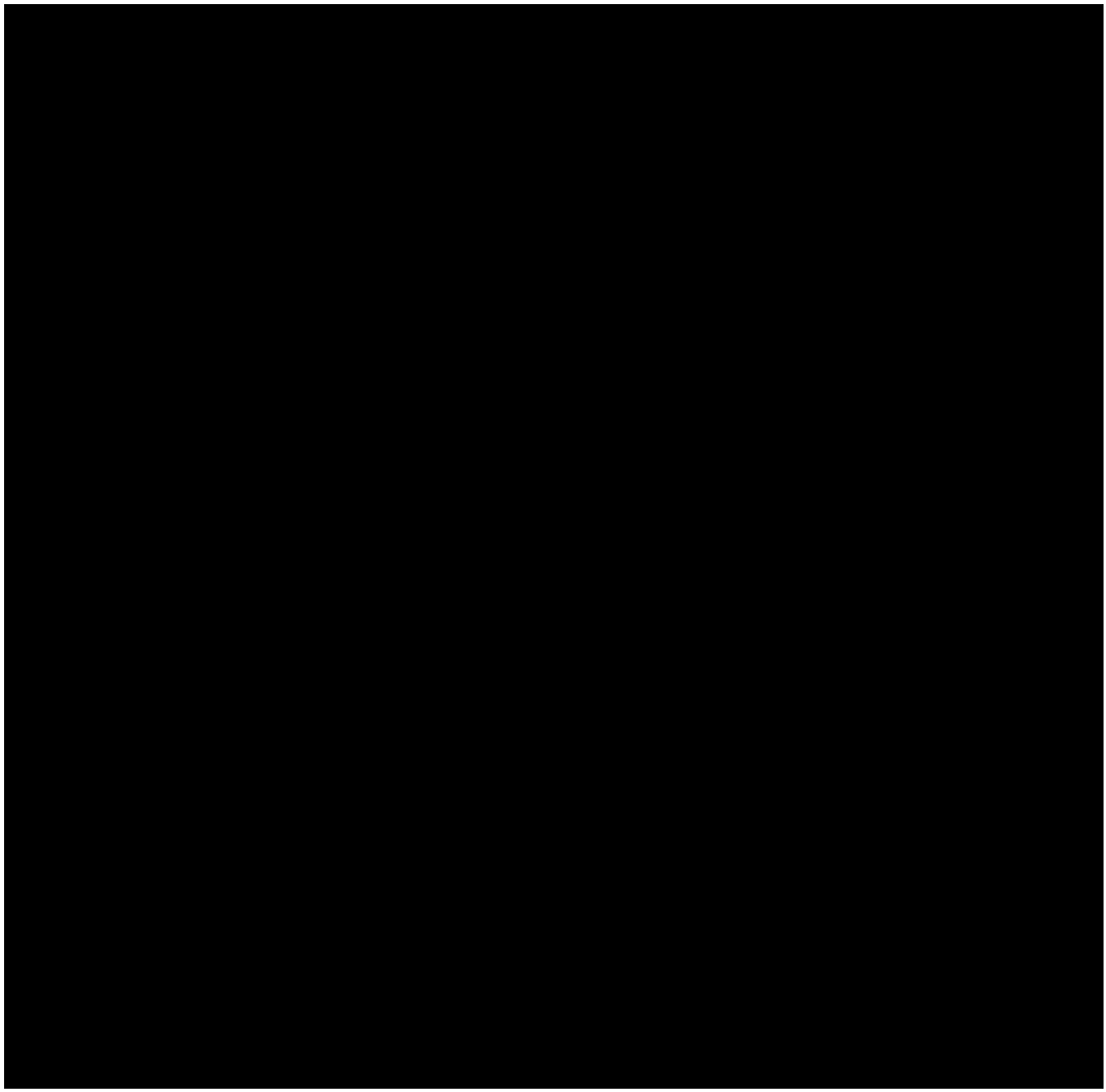


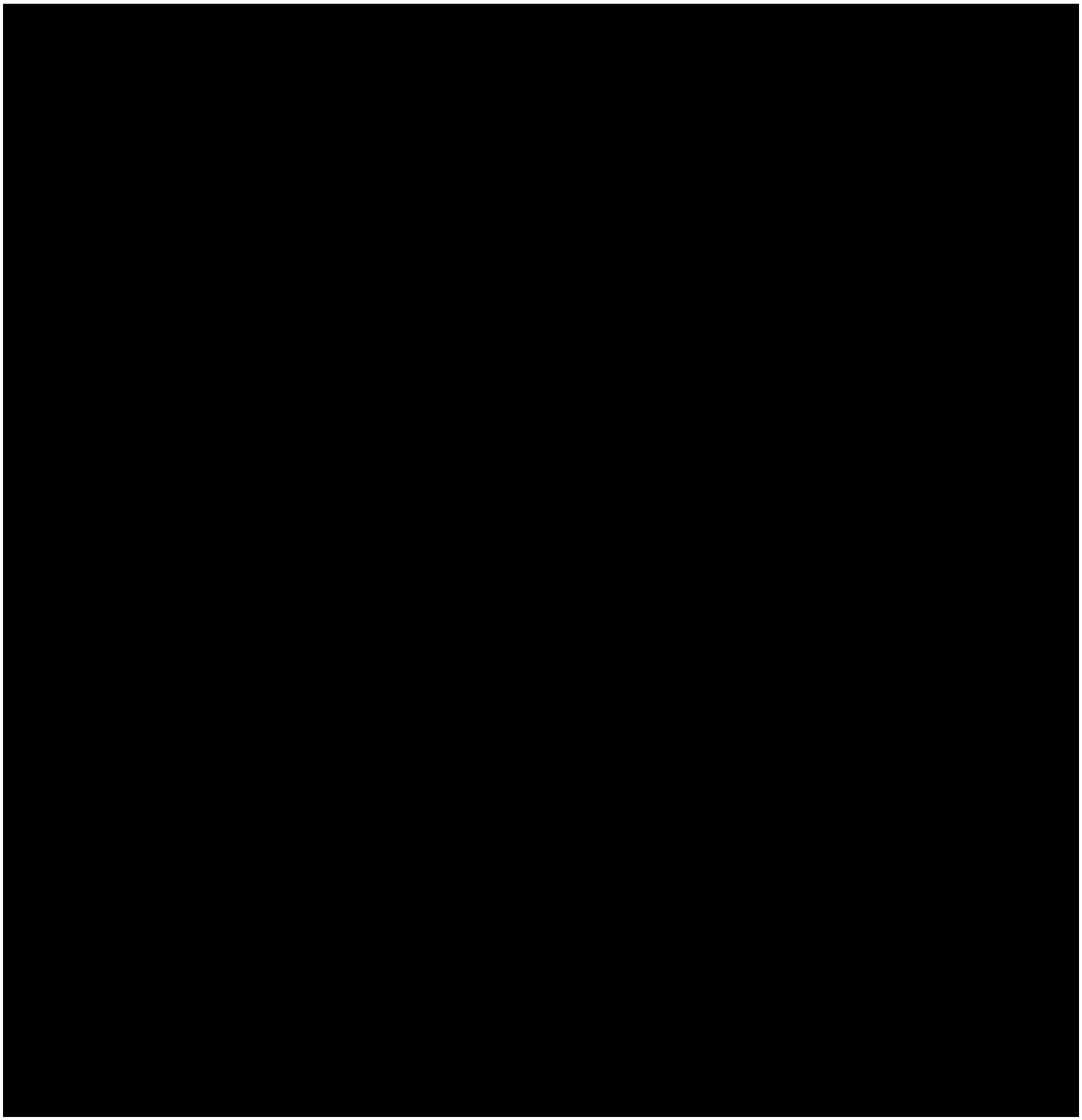


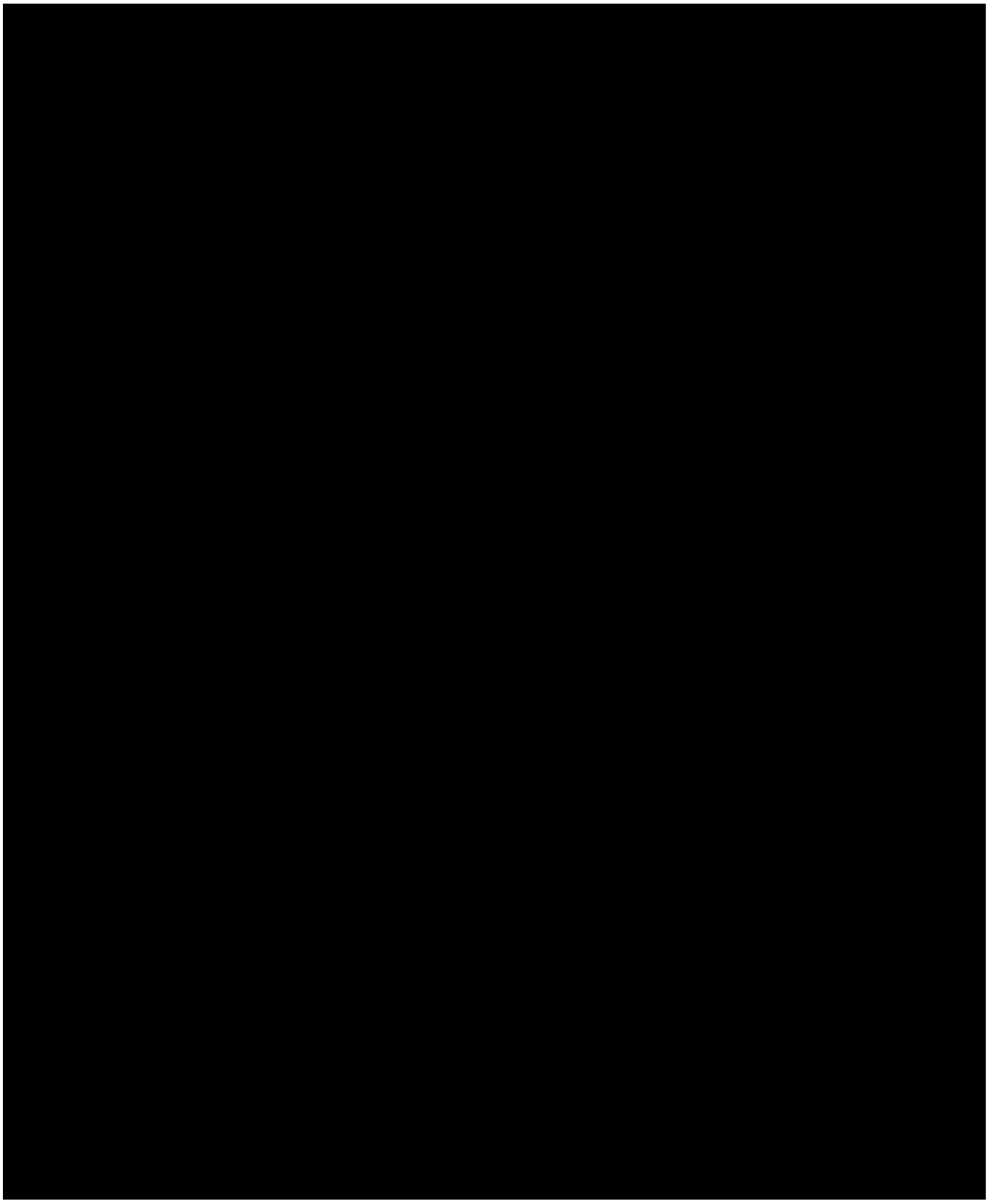


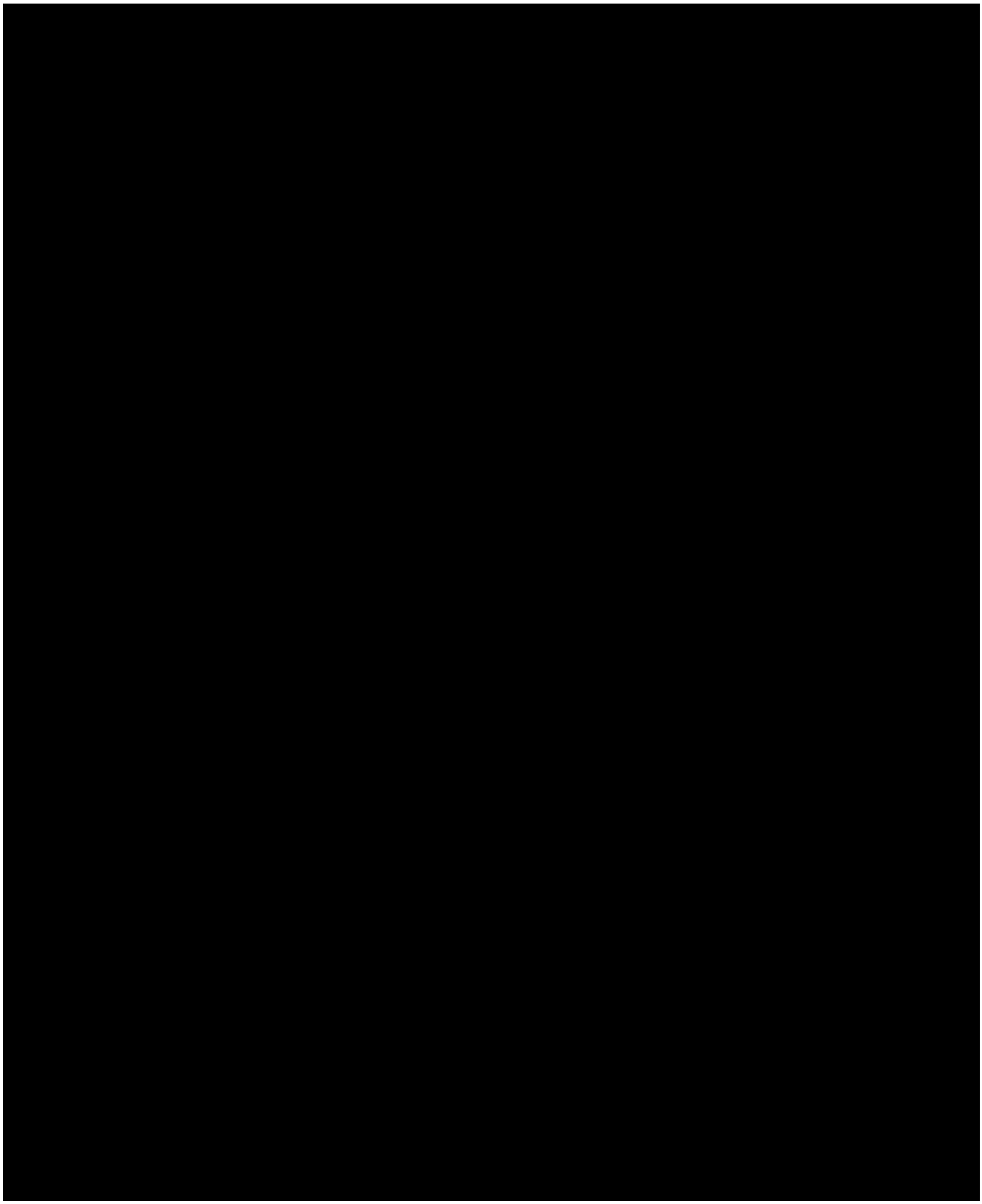


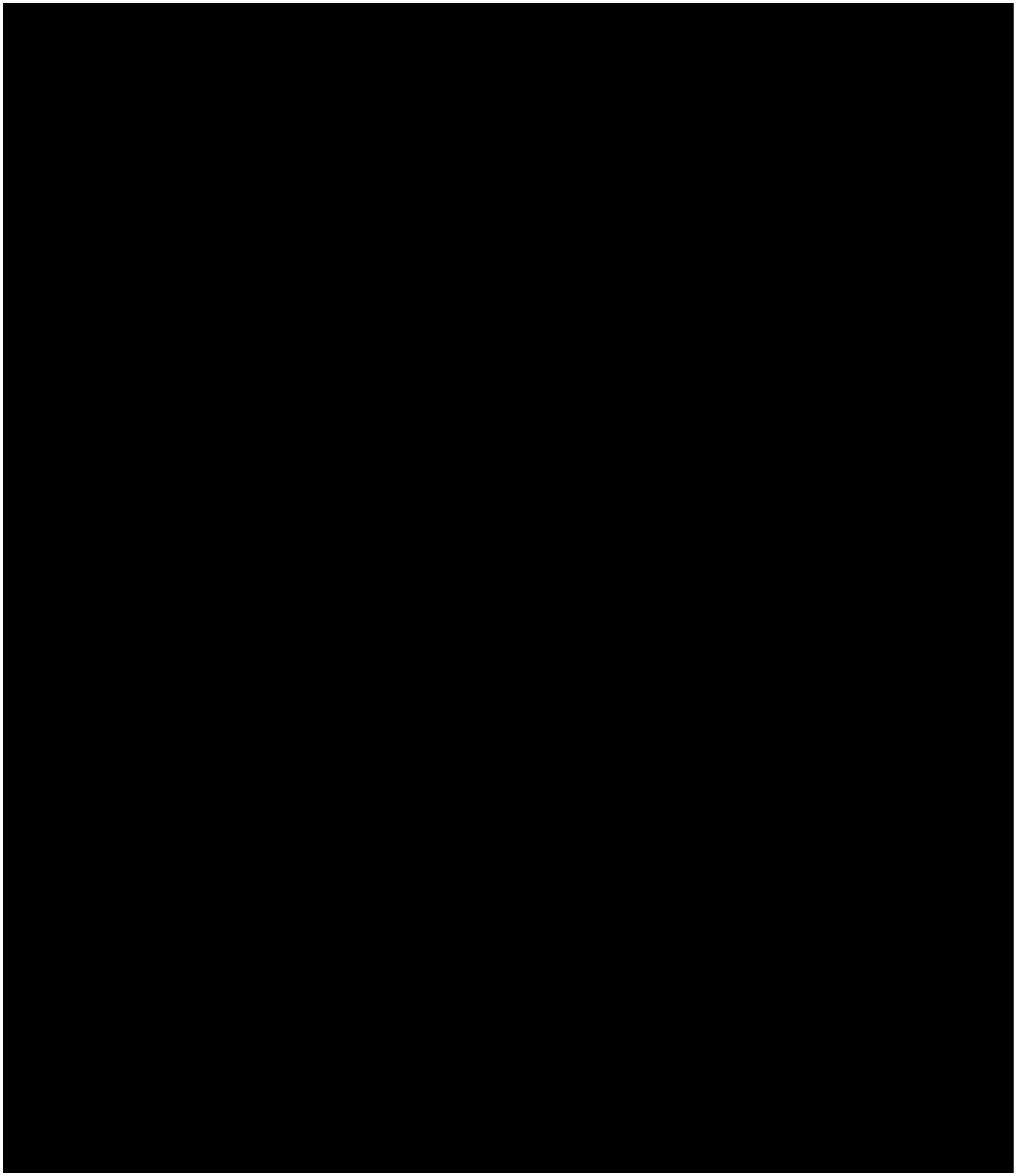


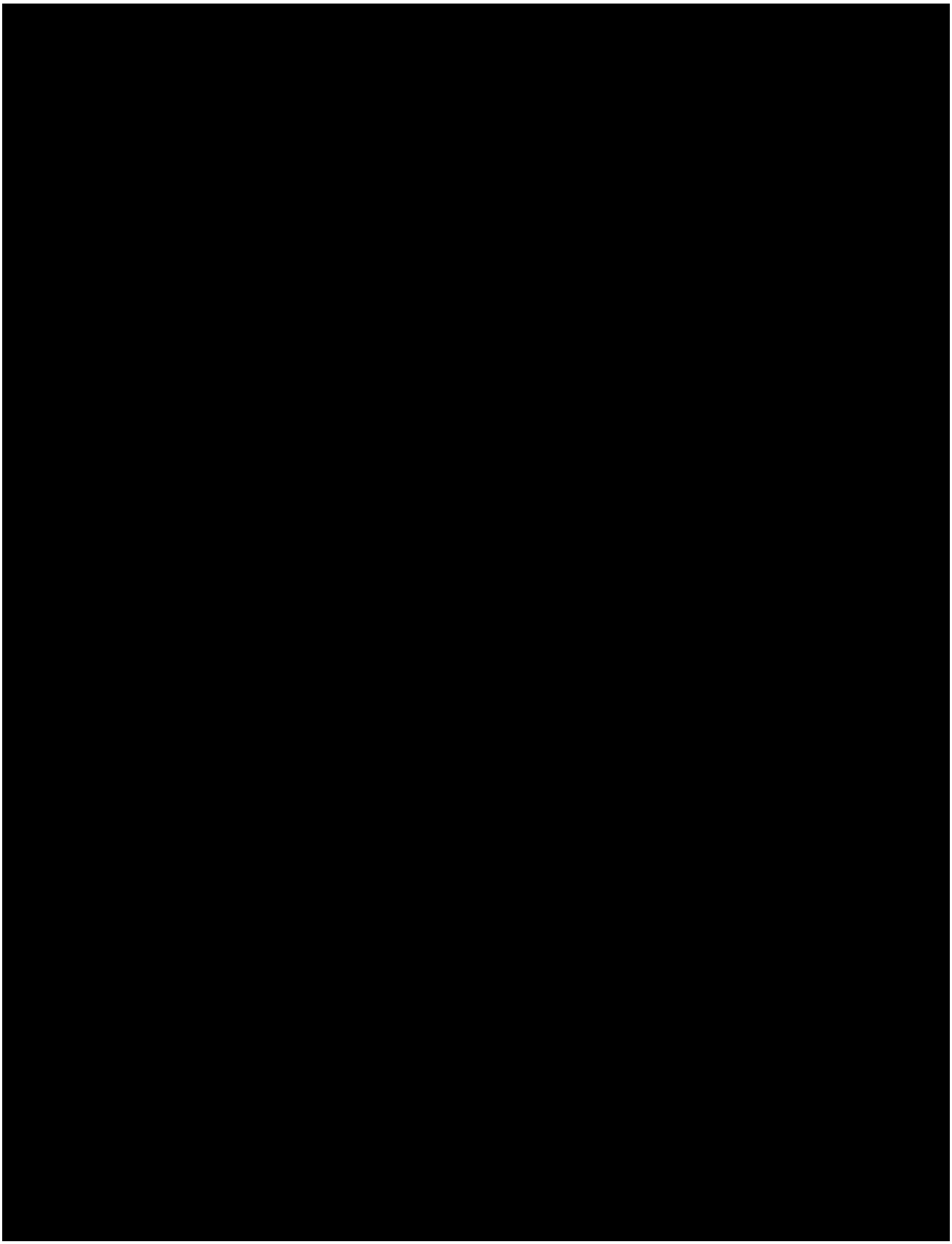


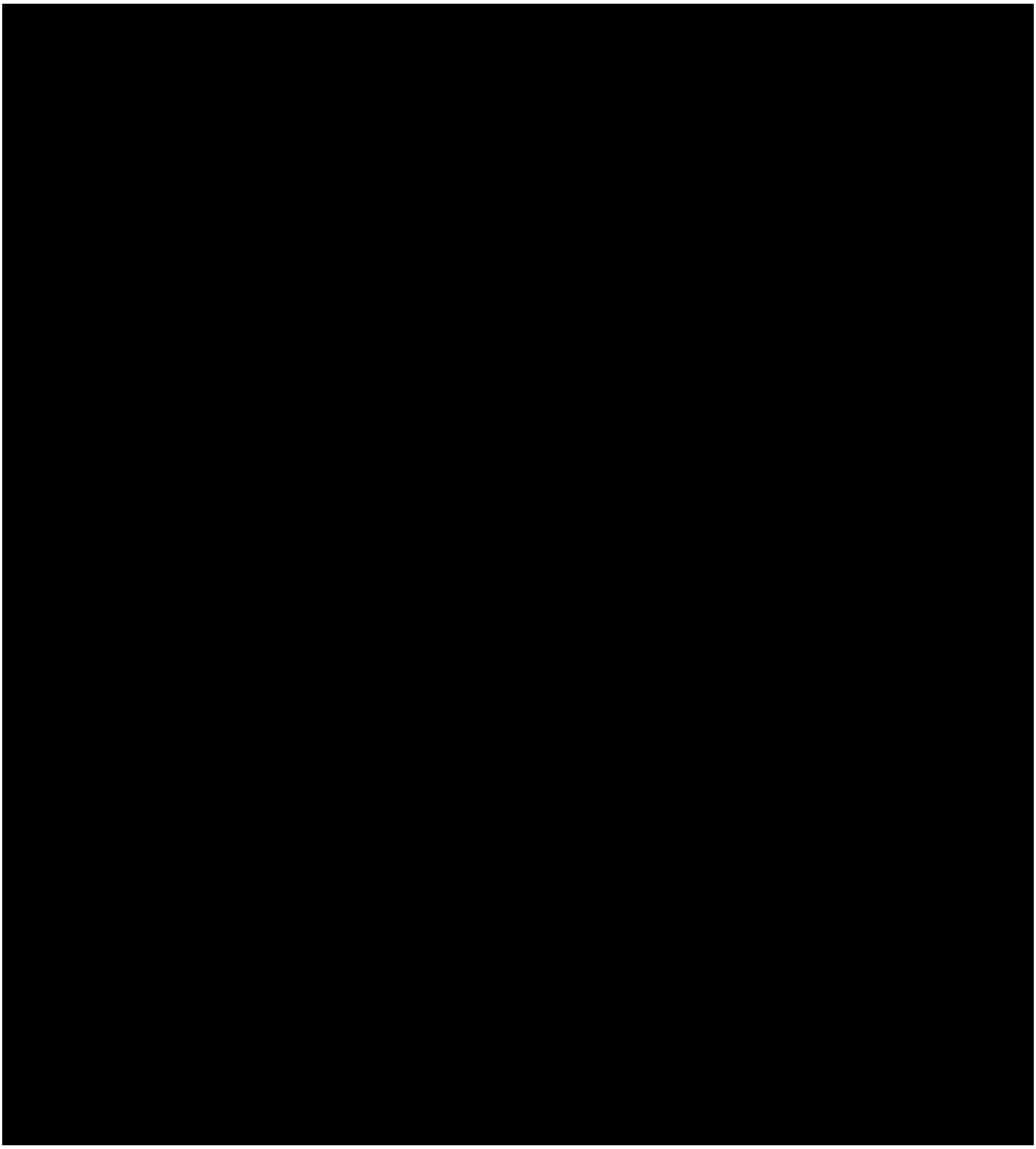




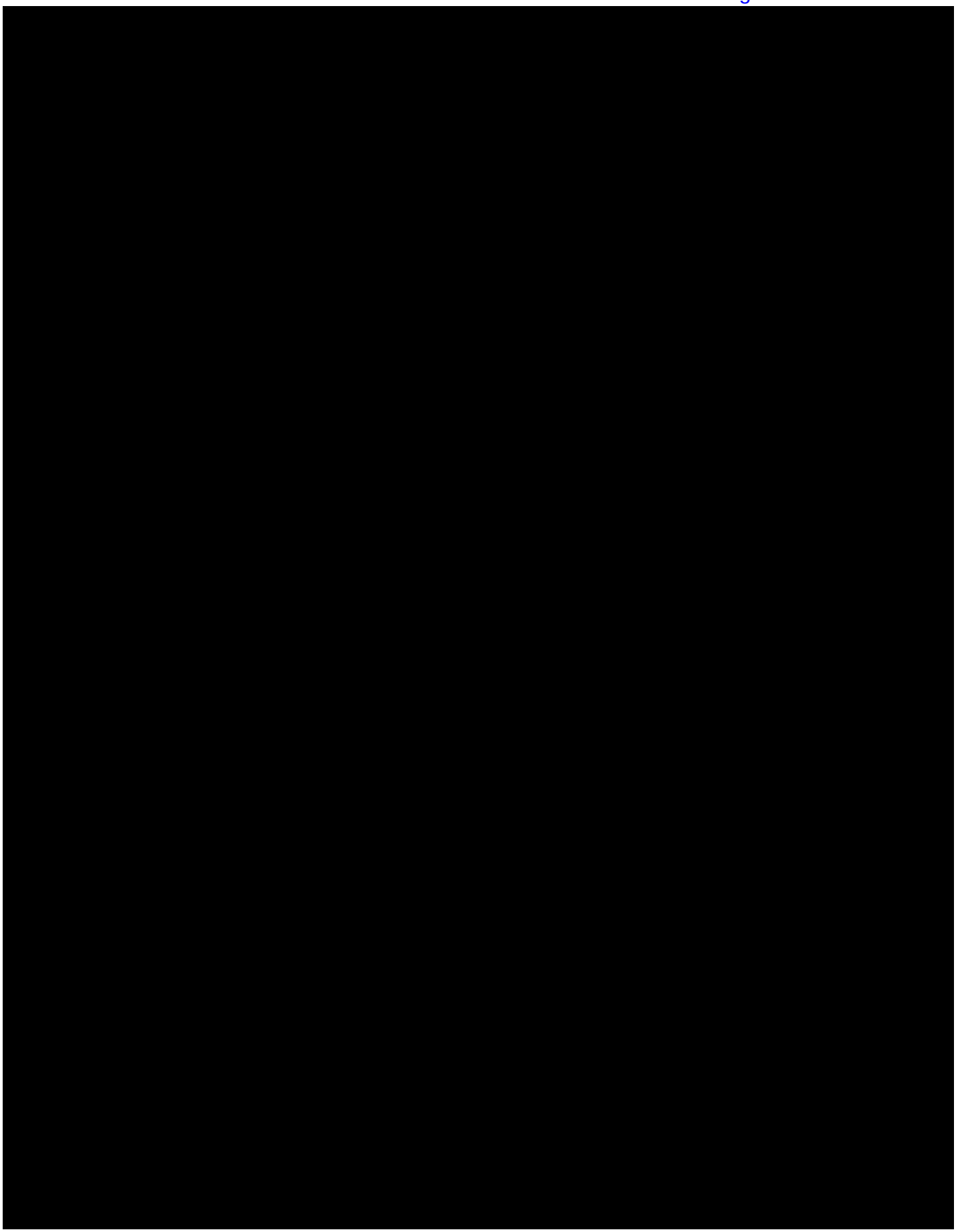


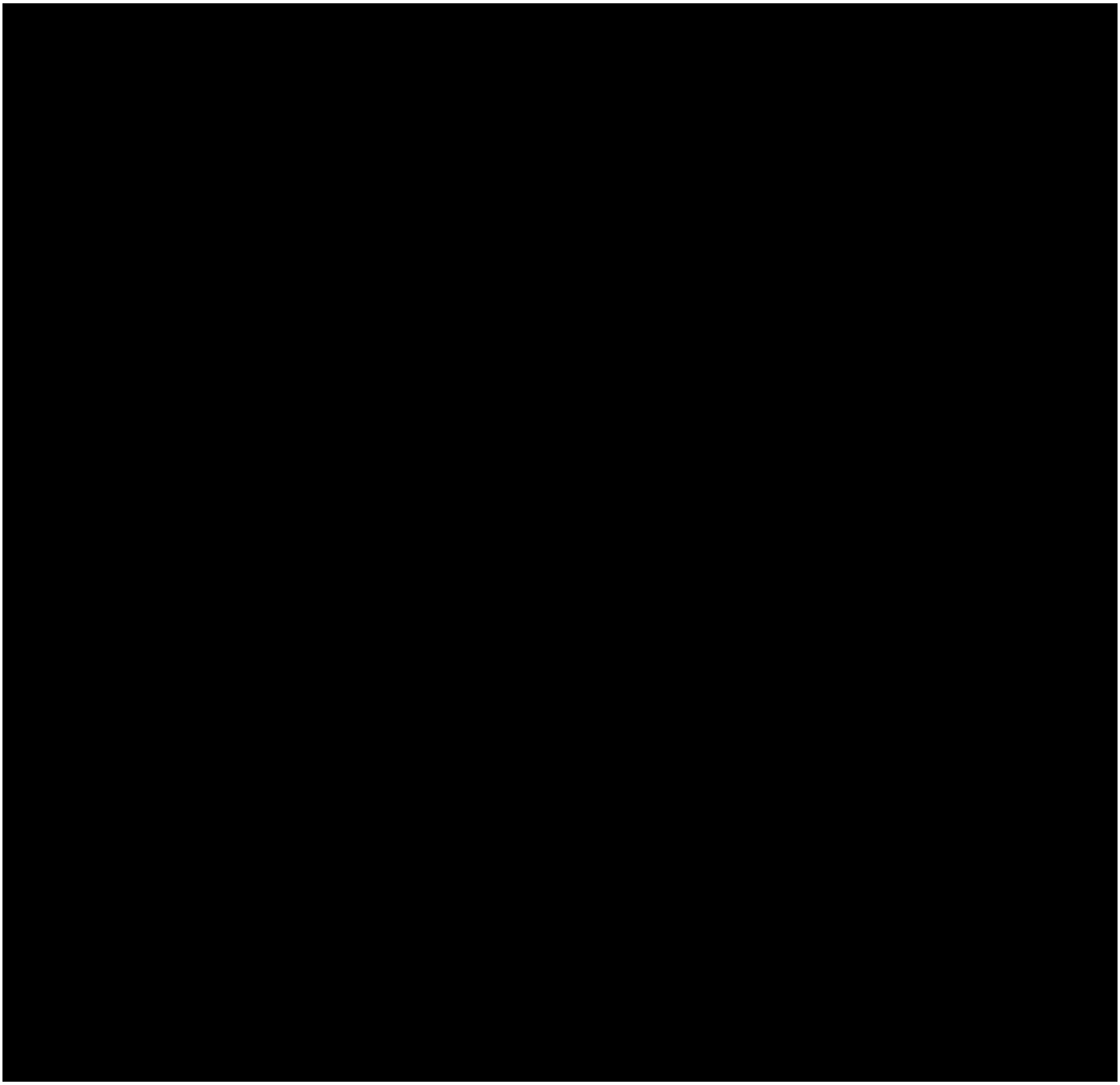




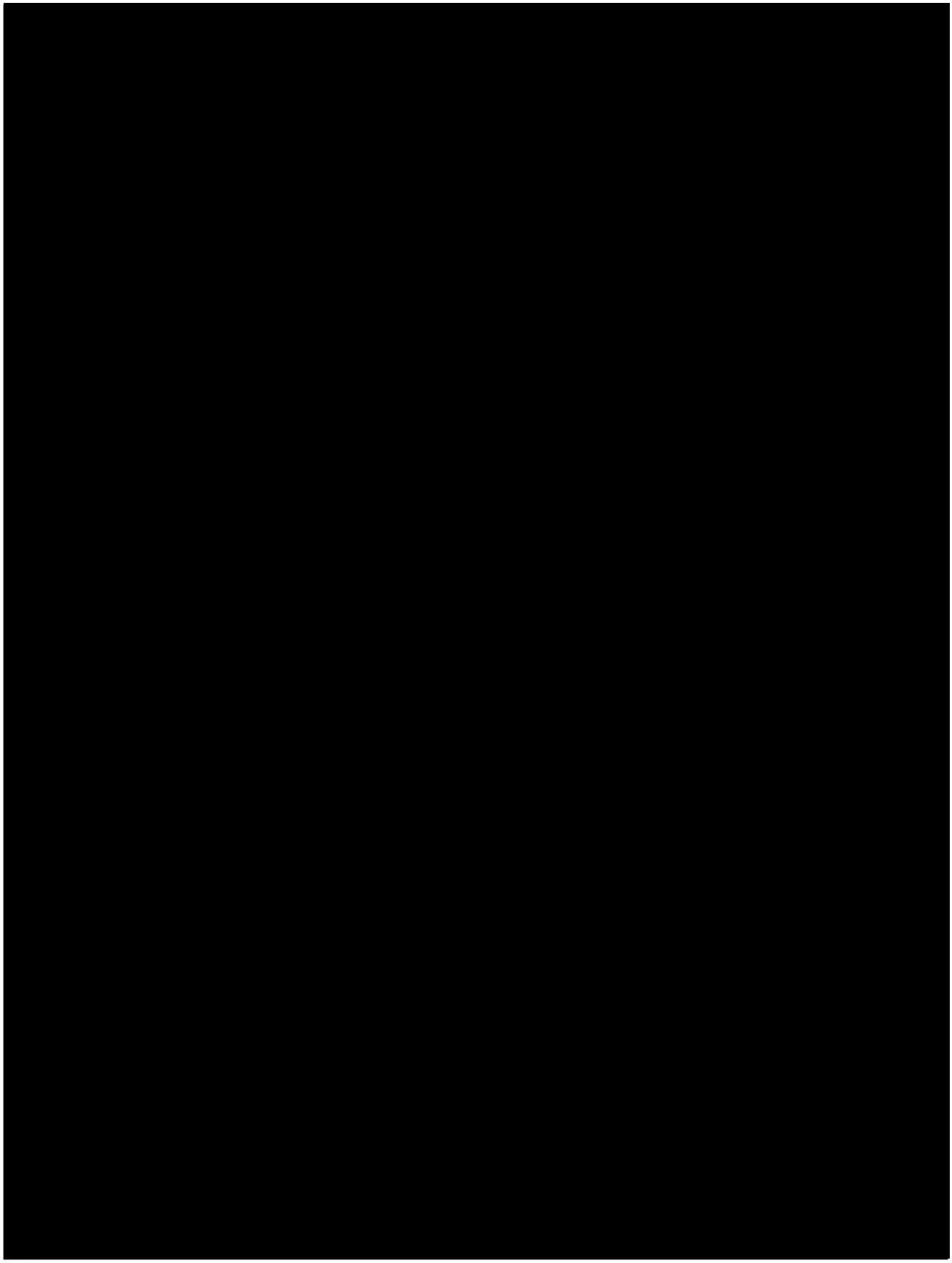


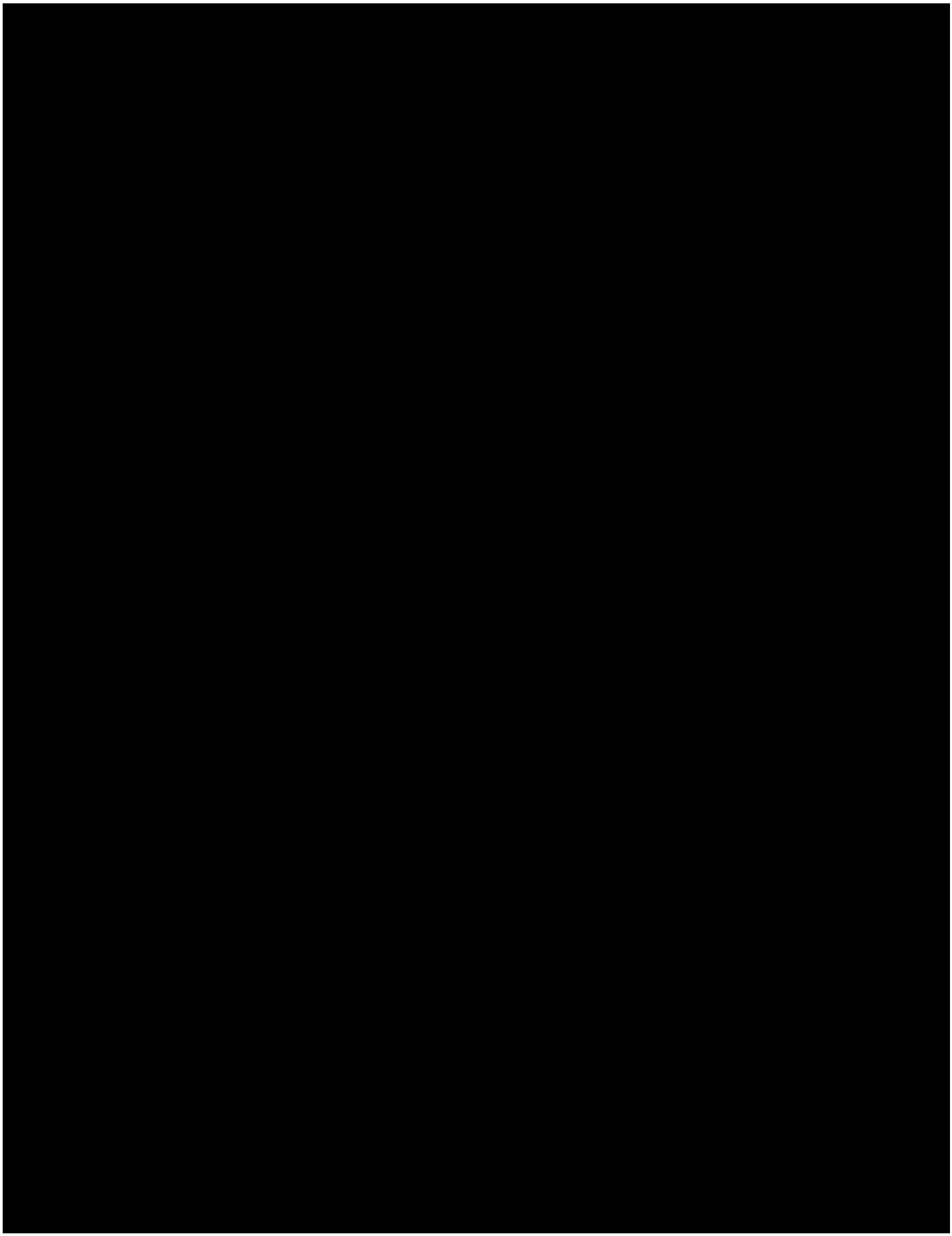
[redacted]

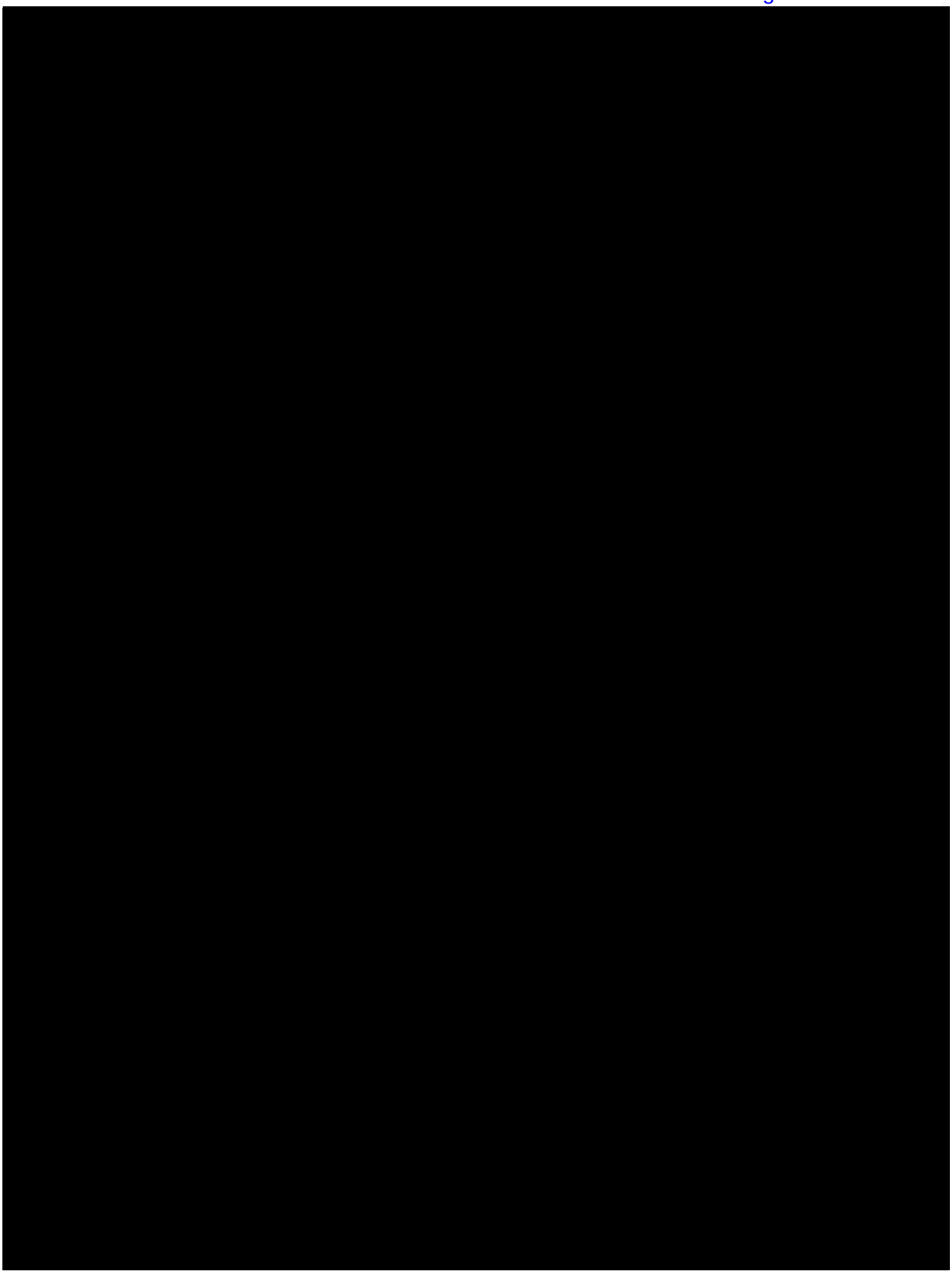


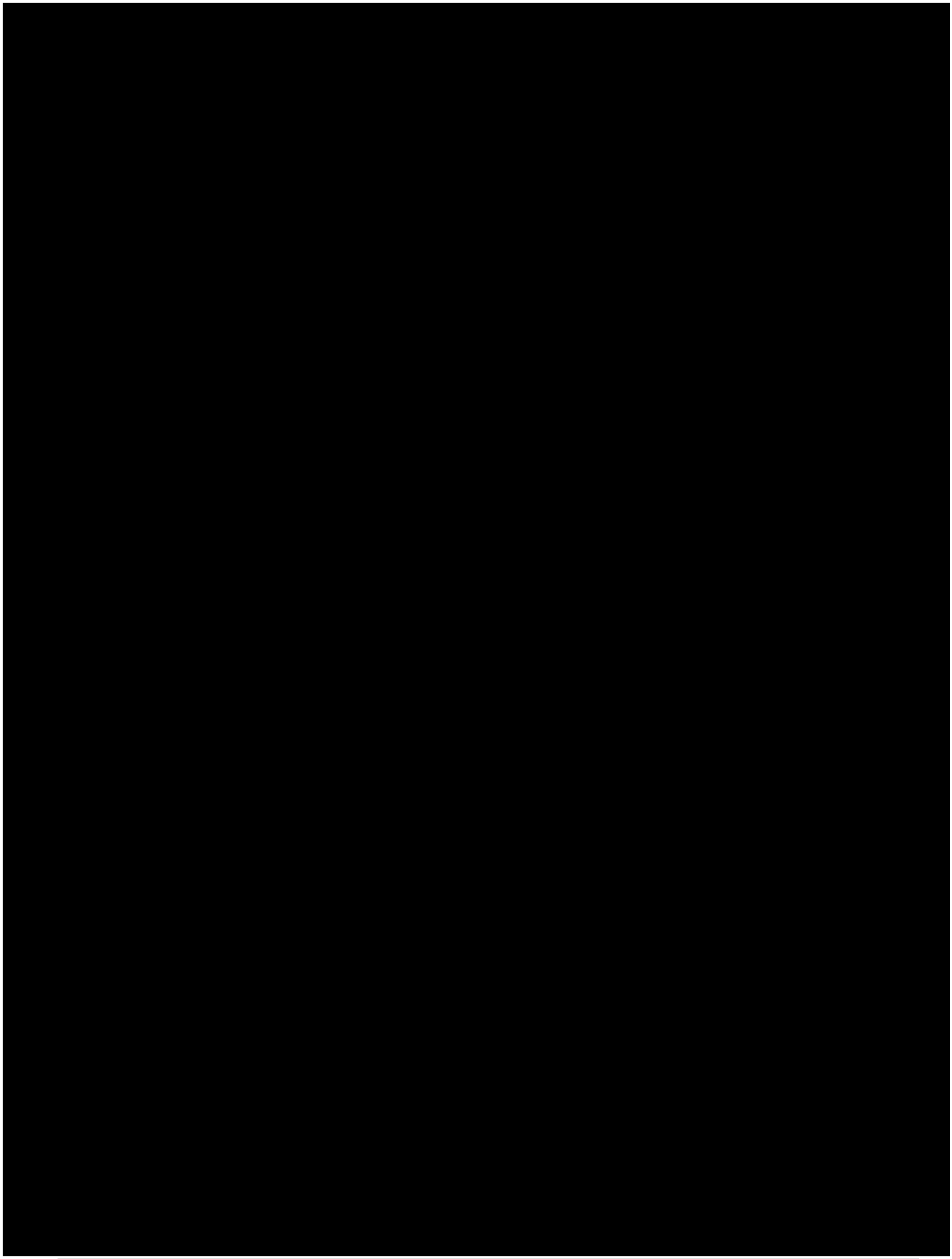


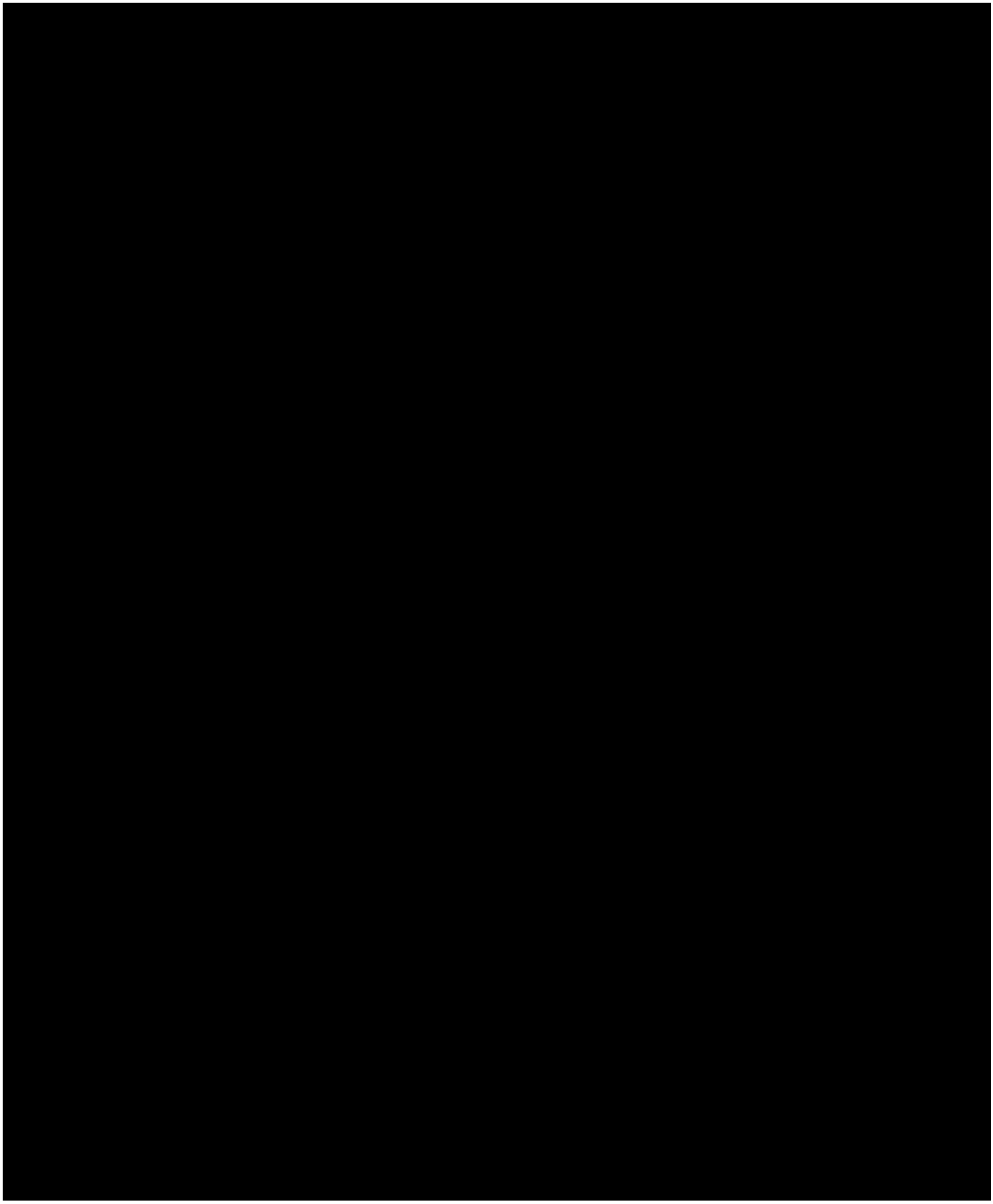
4. SECURITY POLICY IMPLEMENTATION

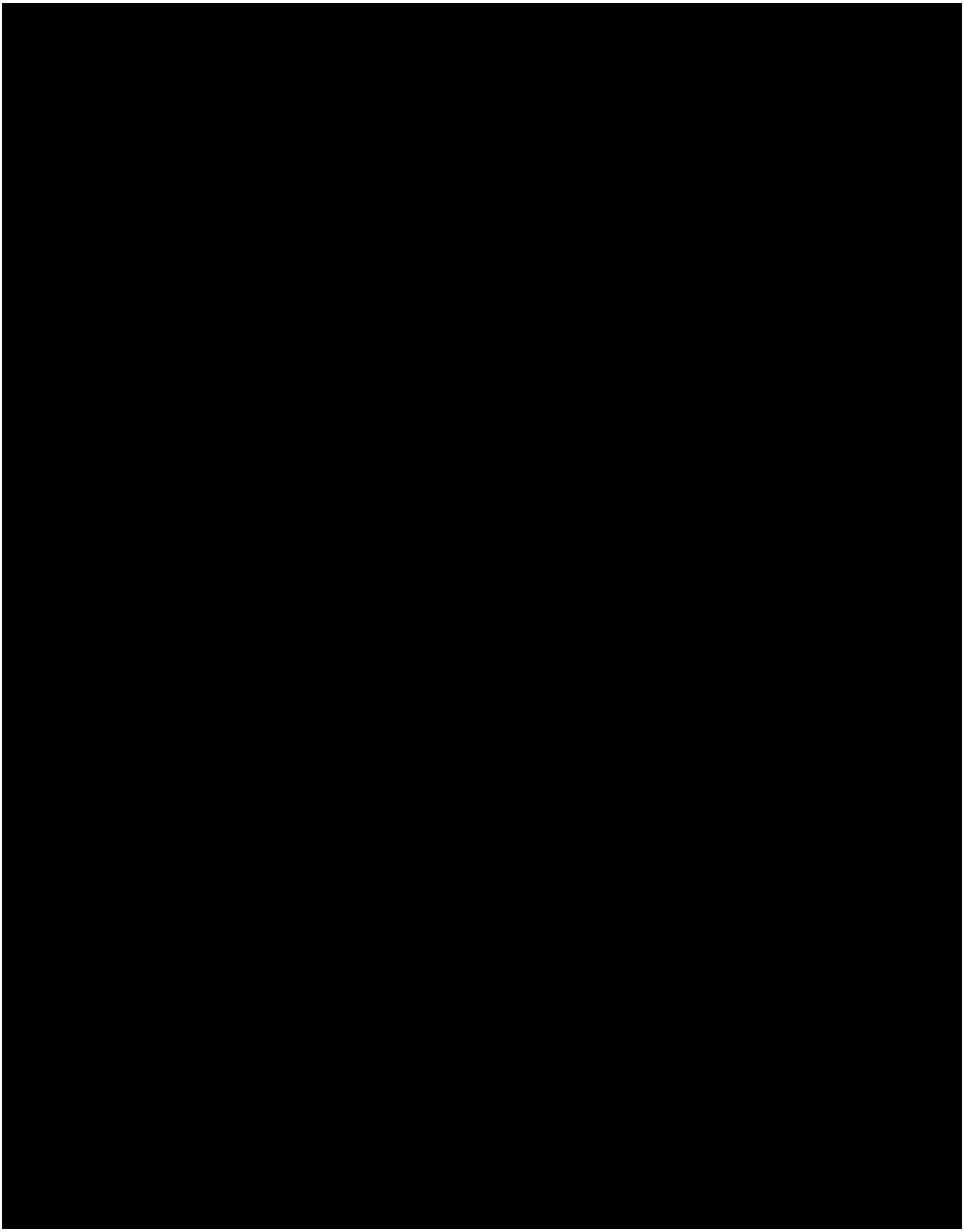


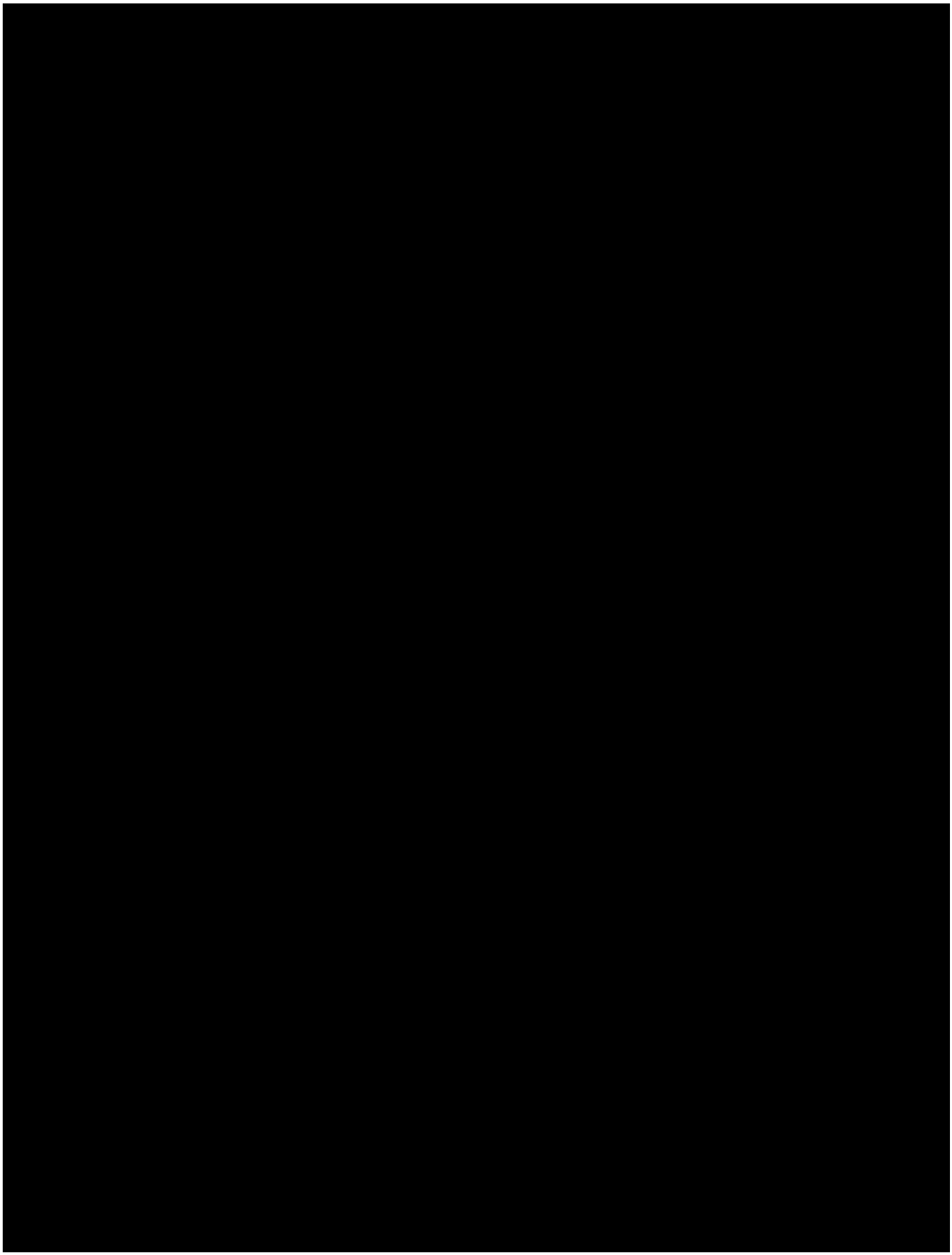


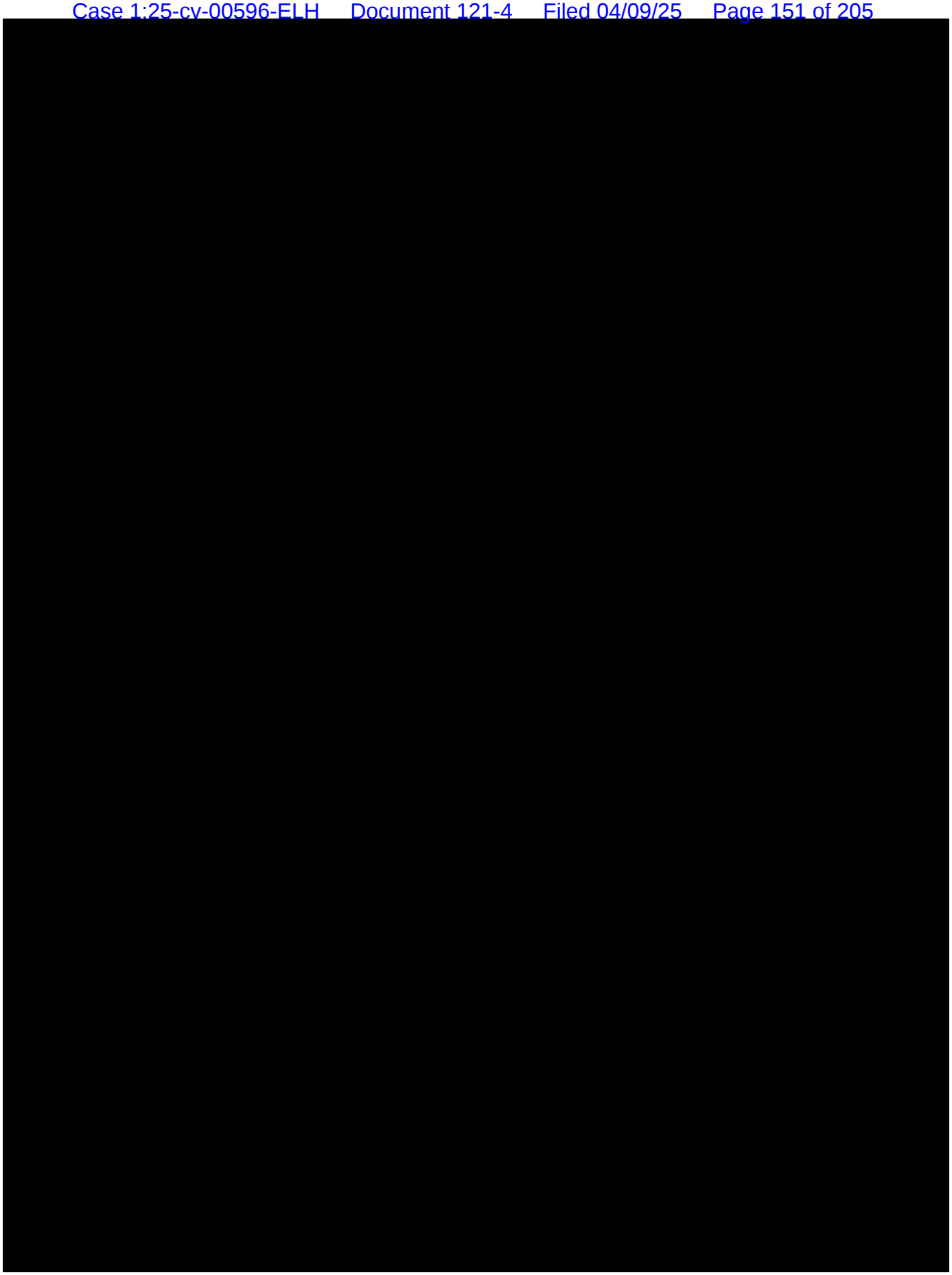


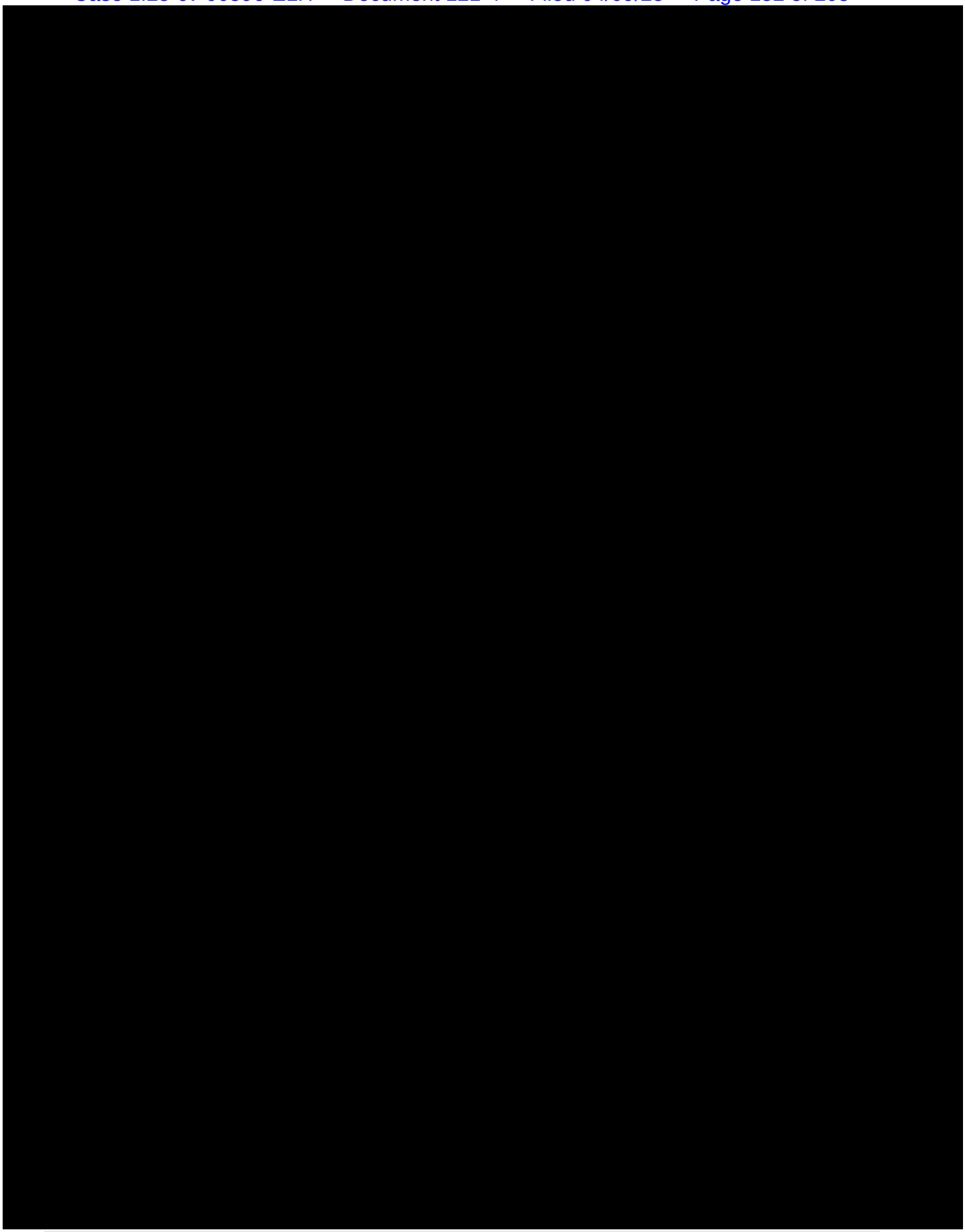


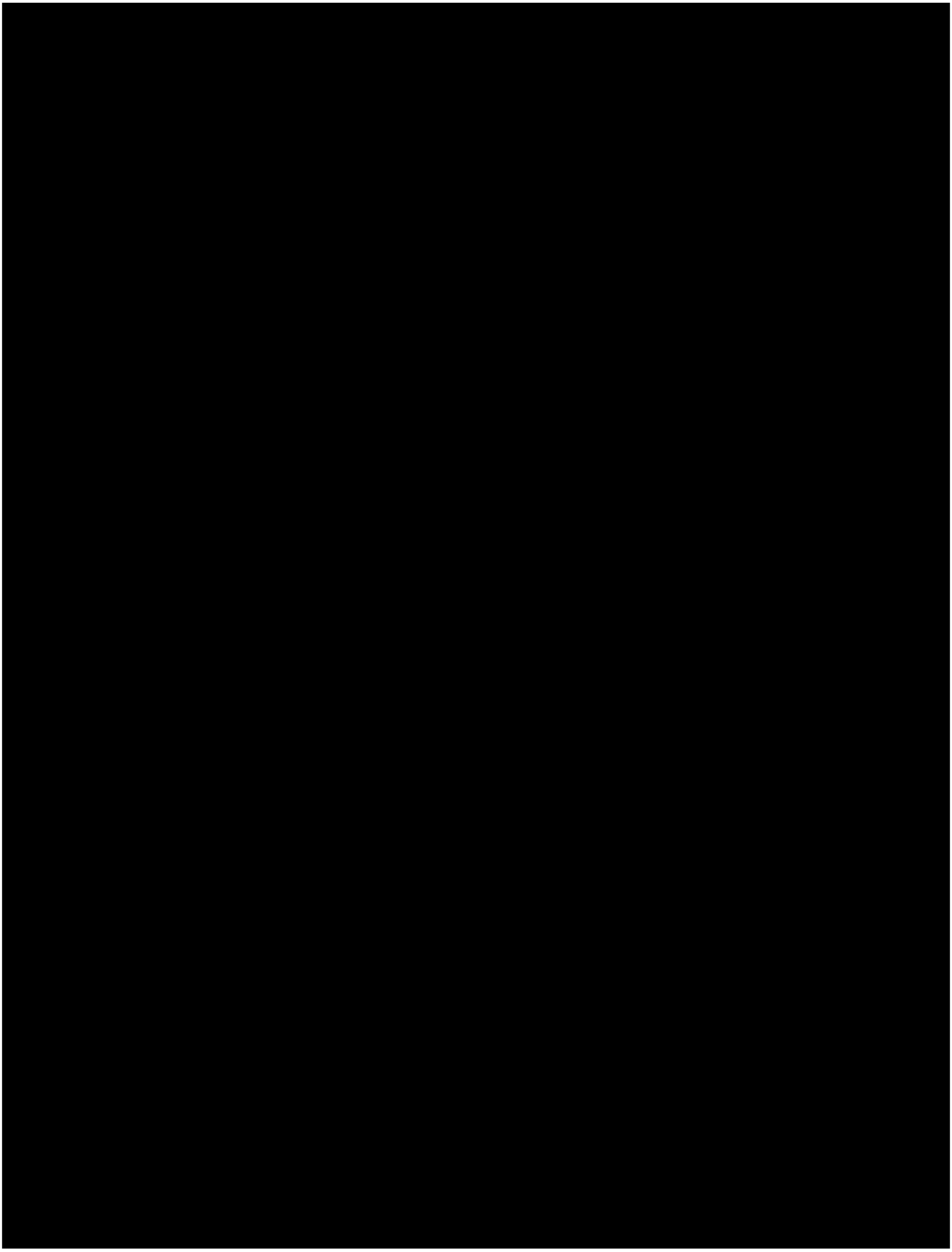


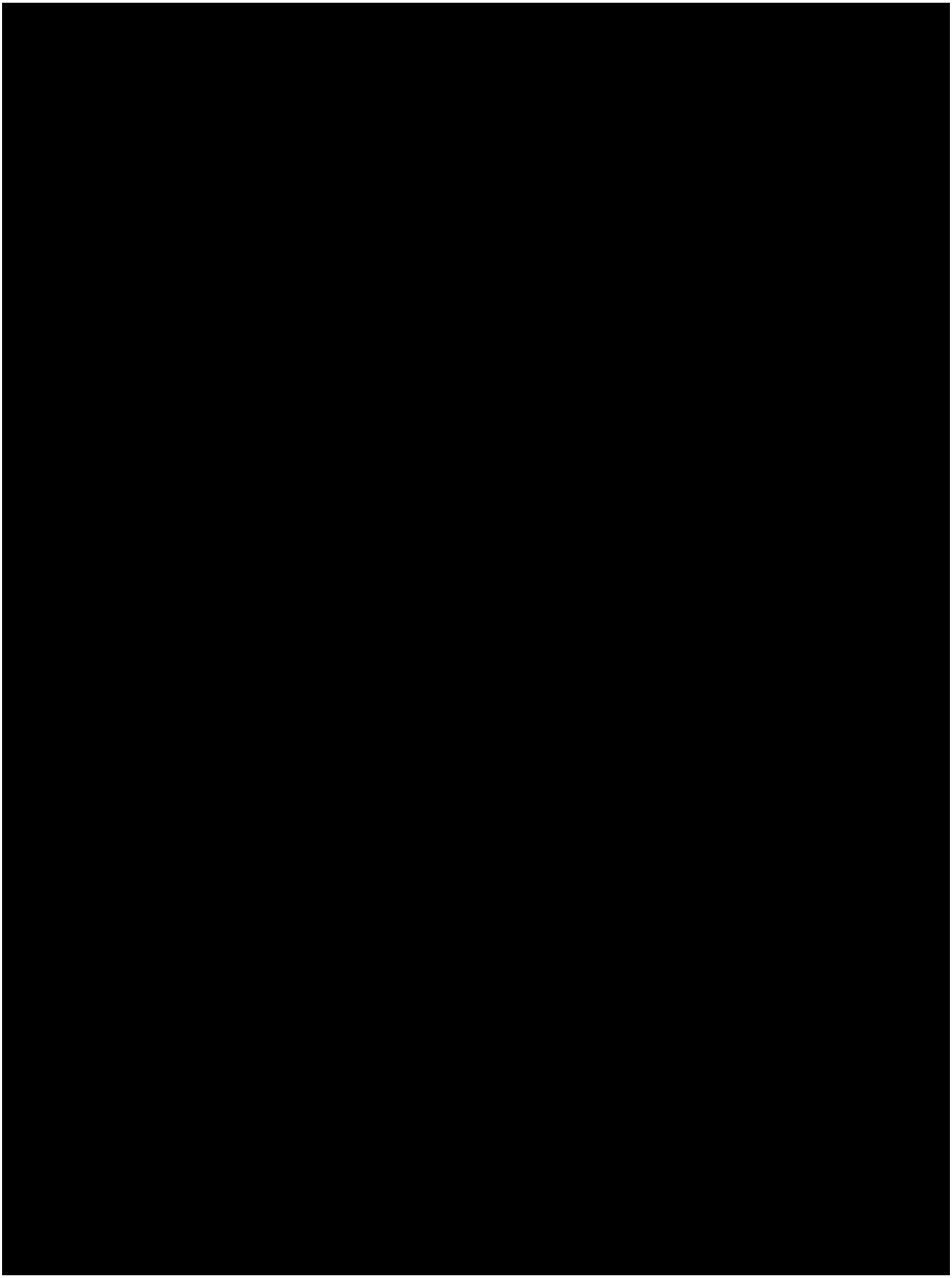


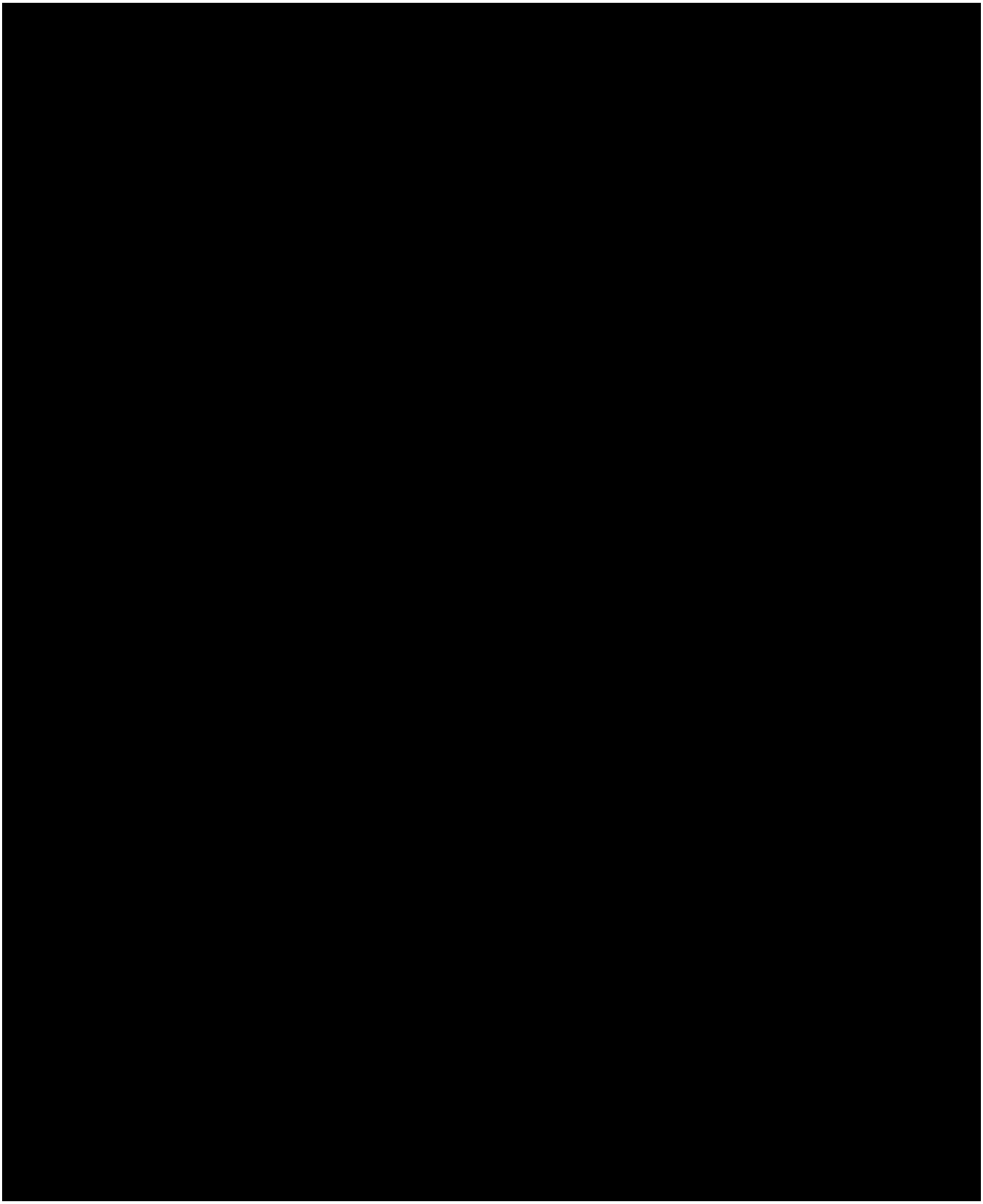


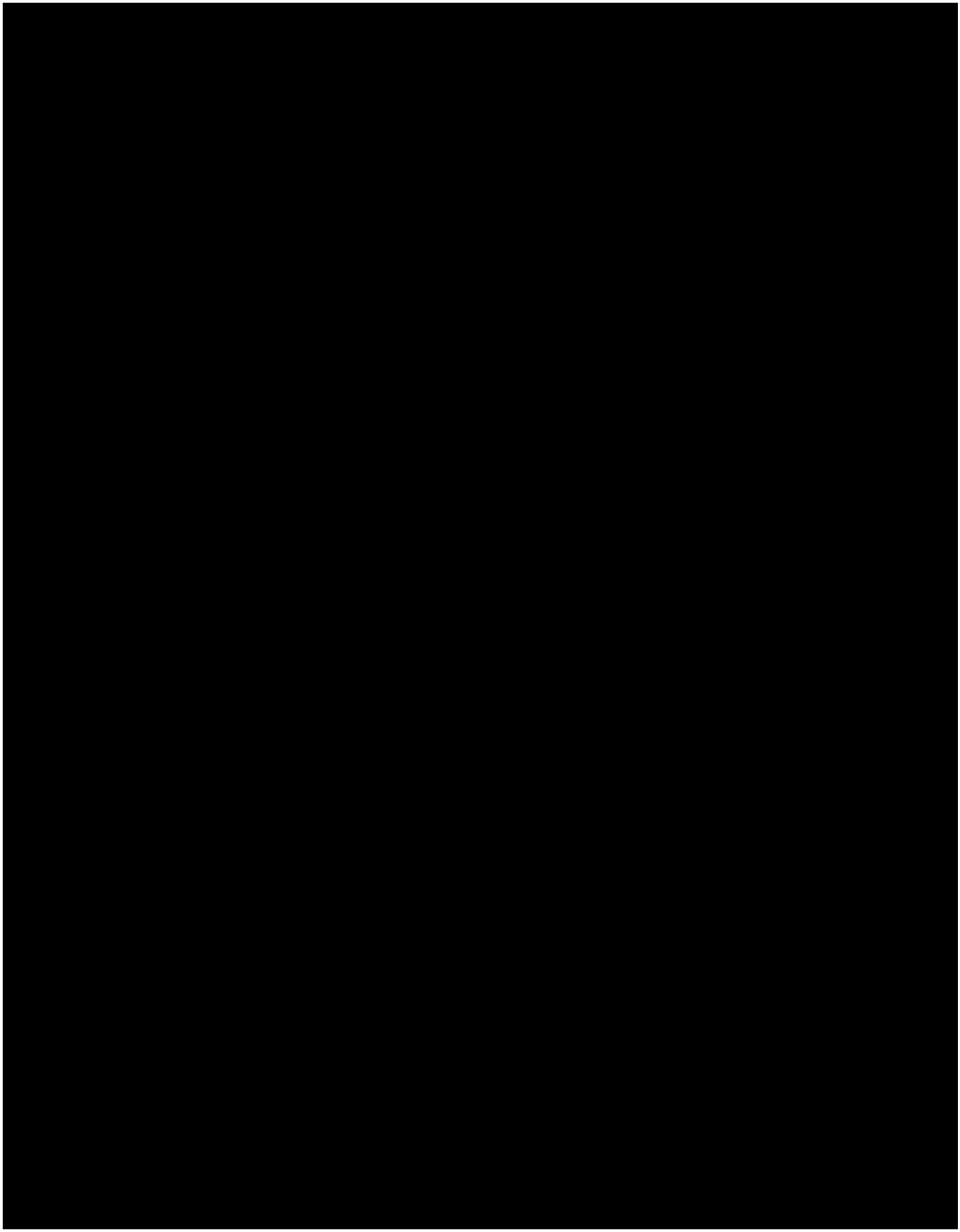












5. INFORMATION SECURITY TRAINING AND AWARENESS

[redacted]

5.1 Information Security Awareness

[redacted]

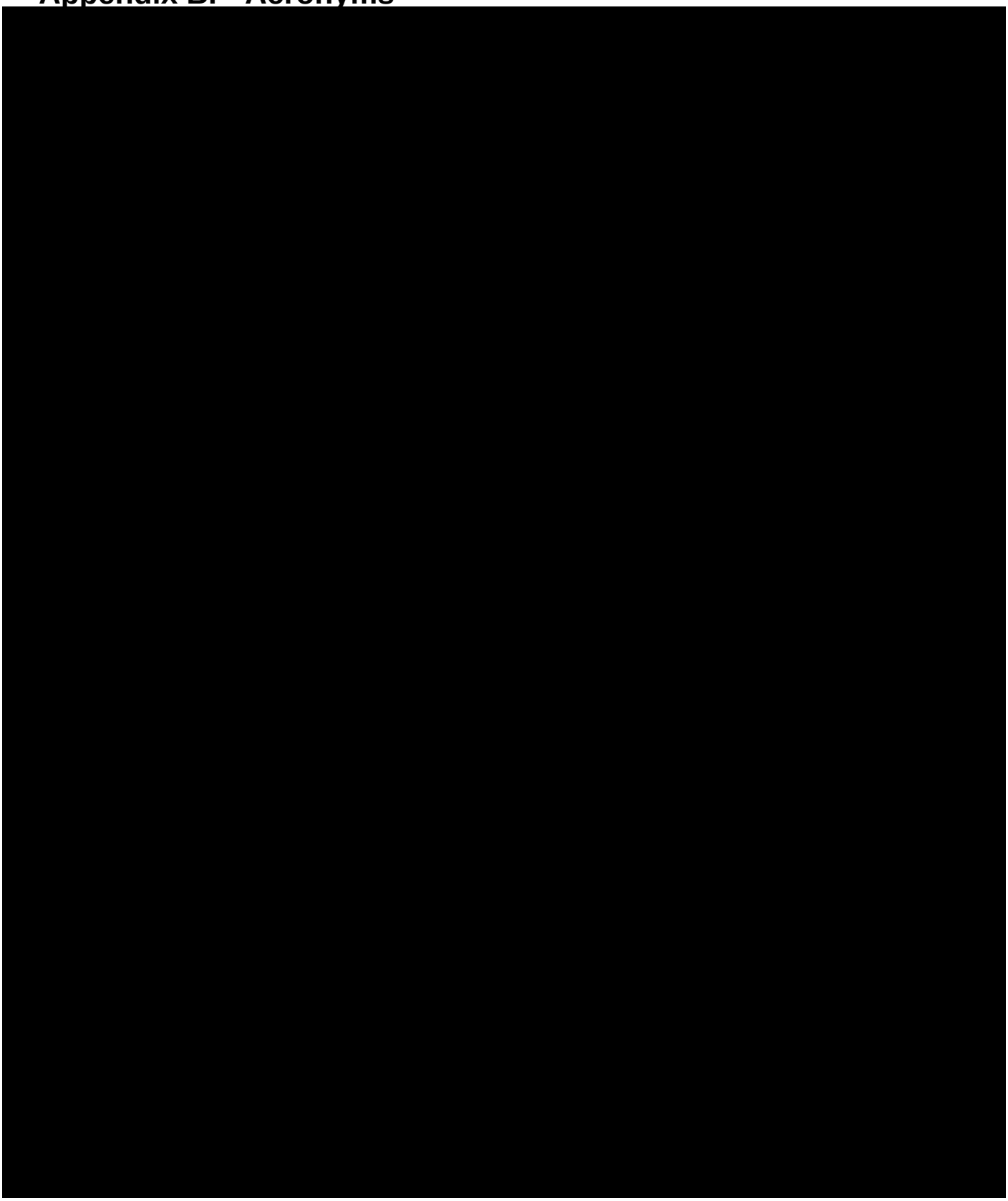
[redacted]

5.2 Systems Security Training

[redacted]

Appendix A. Security Links and References

Appendix B. Acronyms



INFORMATION SECURITY

POLICY (ISP)

FOR

THE SOCIAL SECURITY ADMINISTRATION (SSA)

OFFICE OF INFORMATION SECURITY

OCTOBER 21, 2024

VERSION 9.6.1

SENSITIVE: Internal SSA USE ONLY, Controlled Technical Information (CUI//SP-CTI).

CUI

ATTENTION

Use this space to indicate categories, limited dissemination controls, special instructions, points of contact, etc., if needed.

SENSITIVE

Internal SSA USE ONLY, Controlled Technical Information (CUI//SP-CTI).

ATTENTION

All individuals handling this information are required to protect it from unauthorized disclosure.

Handling, storage, reproduction, and disposition of the attached document(s) must be in accordance with 32 CFR Part 2002 and applicable agency policy.

Access to and dissemination of Controlled Unclassified Information shall be allowed as necessary and permissible to any individual(s), organization(s), or grouping(s) of users, provided such access or dissemination is consistent with or in furtherance of a Lawful Government

CUI

REVISION HISTORY

Use the table in this section to track revisions to the chapter. They will be added to the document Revision History page located in the beginning of the document after the Table of Contents. Leave blank any column for which you are unsure of content (i.e., if you are not the Reviewer / Approver, you would leave the last 3 columns blank).

Version	Revision Date	Brief Description	Author(s)	Last Reviewed Date	Reviewed / Approved by	Effective Date
1.0	01/11/2019	[redacted]	Accenture	NA	Policy Team	01/11/2019
1.1	01/18/2019		Accenture	NA	Policy Team	01/18/2019
1.2	01/28/2019		Accenture	NA	Policy Team	01/28/2019

INFORMATION SECURITY POLICY (ISP)

		[redacted]			
1.3	02/04/2019		02/04/2019	[redacted]	02/04/2019
1.4	02/06/2019		02/06/2019	[redacted]	02/06/2019
1.5	02/07/2019		02/07/2019	[redacted]	02/07/2019
1.6	02/13/2019		02/13/2019	[redacted]	02/13/2019
1.7	03/07/2019		03/07/2019	[redacted]	03/07/2019

INFORMATION SECURITY POLICY (ISP)

		[redacted]			
1.8	03/11/2019		03/11/2019	[redacted]	03/11/2019
1.9	04/01/2019		03/29/2019	[redacted]	04/01/2019

2.0	05/08/2019	[redacted]	05/08/2019	05/08/2019
2.1	05/17/2019		05/17/2019	05/17/2019
2.2	05/22/2019		05/22/2019	05/22/2019
2.3	06/18/2019		06/14/2019	06/18/2019

INFORMATION SECURITY POLICY (ISP)

		[redacted]			
2.4	08/01/2019		08/02/2019	[redacted]	08/02/2019
2.5	08/22/2019		08/22/2019		08/22/2019
2.6	09/18/2019		09/18/2019		09/18/2019

INFORMATION SECURITY POLICY (ISP)

2.7	09/26/2019	[redacted]	[redacted]	09/26/2019	[redacted]	09/26/2019
2.8	10/10/2019		[redacted]	10/04/2019	[redacted]	10/10/2019
2.9	10/16/2019		[redacted]	10/16/2019	[redacted]	10/16/2019
3.0	11/18/2019		[redacted]	11/18/2019	[redacted]	11/18/2019
3.1	11/25/2019		Policy Team	11/25/2019	[redacted]	11/25/2019
3.2	12/02/2019		Policy Team	11/29/2019	[redacted]	12/02/2019

INFORMATION SECURITY POLICY (ISP)

		[redacted]				
3.3	12/04/2019		Policy Team	12/04/2019	[redacted]	12/04/2019
3.4	12/18/2019		Policy Team [redacted]	12/17/2019	[redacted]	12/18/2019
3.5	12/31/2019		[redacted]	12/31/2019	[redacted]	12/31/2019

3.6	01/10/2020	[redacted]	01/10/2020	[redacted]	01/10/2020
3.7	01/24/2020		01/24/2020		01/24/2020
3.8	02/05/2020		02/05/2020		02/05/2020
3.9	03/06/2020		02/13/2020		03/06/2020
4.0	03/11/2020	Policy Team Accenture	03/10/2020		03/11/2020

INFORMATION SECURITY POLICY (ISP)

		[redacted]		[redacted]	
4.1	03/24/2020		Policy Team	03/24/2020	03/24/2020
4.2	04/03/2020		[redacted]	04/03/2020	04/03/2020
4.3	04/13/2020		[redacted]	04/13/2020	04/13/2020
4.4	04/27/2020		[redacted] Accenture	04/27/2020	04/27/2020

		[redacted]				
4.5	04/30/2020		Policy Team	04/30/2020	[redacted]	04/30/2020
4.6	05/07/2020		Accenture Policy Team	05/07/2020		05/07/2020

INFORMATION SECURITY POLICY (ISP)

		[redacted]				
4.7	05/13/2020		Policy Team	05/13/2020	[redacted]	05/13/2020
4.8	05/22/2020		[redacted] Policy Team	05/22/2020	[redacted]	05/22/2020
4.9	06/08/2020		Policy Team	06/08/2020	[redacted]	06/08/2020
5.0	06/11/2020		[redacted] Accenture	06/10/2020	[redacted]	06/11/2020

INFORMATION SECURITY POLICY (ISP)

5.1	06/25/2020	Policy Team Accenture	06/24/2020		06/25/2020
5.2	06/26/2020	[redacted]	06/25/2020		06/26/2020
5.3	07/10/2020	Policy Team	07/10/2020		07/10/2020
5.4	07/15/2020	[redacted]	07/15/2020		07/15/2020
5.5	08/14/2020	[redacted]	08/14/2020		08/14/2020

INFORMATION SECURITY POLICY (ISP)

5.6	09/03/2020	[redacted]	09/04/2020	09/04/2020
5.7	09/05/2020		10/05/2020	10/05/2020
5.8	11/09/2020		11/09/2020	11/09/2020

5.9	11/17/2020	[redacted]	11/17/2020	11/17/2020
6.0	11/19/2020		11/17/2020	11/19/2020

INFORMATION SECURITY POLICY (ISP)

6.1	12/22/2020	[redacted]	12/22/2020	12/22/2020
6.2	01/11/2021		01/11/2021	01/11/2021
6.3	02/01/2021		02/01/2021	02/01/2021
6.4	02/22/2021		02/22/2021	02/22/2021

6.5	03/04/2021	[redacted]	03/04/2021	03/04/2021
6.6	03/12/2021		03/12/2021	03/12/2021
6.7	03/31/2021		03/31/2021	03/31/2021
6.8	04/15/2021		04/15/2021	04/15/2021

INFORMATION SECURITY POLICY (ISP)

		[redacted]				
6.9	05/20/2021		[redacted]	05/20/2021	[redacted]	05/20/2021
7.0	06/09/2021		[redacted]	06/09/2021	[redacted]	06/09/2021
7.1	06/16/2021		Policy Team	06/16/2021	[redacted]	06/16/2021

INFORMATION SECURITY POLICY (ISP)

7.2	06/22/2021	[redacted]	Policy Team	06/22/2021	[redacted]	06/22/2021
7.3	07/21/2021		[redacted]	07/21/2021	[redacted]	07/21/2021
7.4	07/23/2021		DSE/ Policy Team	07/23/2021	[redacted]	07/23/2021

7.5	08/16/2021	[redacted]	Policy Team	08/13/2021	[redacted]	08/16/2021

7.6	09/24/2021	[redacted]	Policy Team	09/24/2021	[redacted]	09/24/2021
7.7	10/08/2021		Policy Team	10/08/2021	[redacted]	10/08/2021

INFORMATION SECURITY POLICY (ISP)

		[redacted]				
7.8	10/27/2021		Training Team Policy Team	10/26/2021	[redacted]	10/27/2021
7.9	12/16/2021		Policy Team	12/16/2021	[redacted]	12/16/2021
8.0	01/19/2022		Policy Team [redacted]	01/18/2022	[redacted]	01/18/2022
8.1	03/08/2022		[redacted]	03/08/2022	[redacted]	03/08/2022

INFORMATION SECURITY POLICY (ISP)

		[redacted]		
8.2	04/27/2022		04/27/2022	04/27/2022
8.3	05/23/2022		05/23/2022	05/23/2022

		[redacted]				
8.4	08/17/2022		Policy Team	08/17/2022	[redacted]	08/17/2022
8.5	08/29/2022		[redacted]	09/29/2022	[redacted]	09/29/2022

INFORMATION SECURITY POLICY (ISP)

		[redacted]			
8.6	12/12/2022		12/12/2022	[redacted]	12/12/2022
8.7	03/08/2023		03/08/2023		03/08/2023

INFORMATION SECURITY POLICY (ISP)

		[redacted]			
8.8	04/21/2023		04/20/2023	[redacted]	04/20/2023

INFORMATION SECURITY POLICY (ISP)

		[redacted]			
8.9	06/05/2023		06/05/2023	[redacted]	06/05/2023
9.0	08/24/2023		08/24/23		08/22/2023

INFORMATION SECURITY POLICY (ISP)

		[redacted]				
9.1	09/08/2023		[redacted] OIS Policy	09/08/2023	[redacted]	09/08/2023
9.2	09/28/2023		[redacted] OIS Policy	09/08/2023	[redacted]	09/28/2023
9.3	12/18/2023		[redacted] OIS Policy	12/18/2023	[redacted]	12/18/2023

INFORMATION SECURITY POLICY (ISP)

		[redacted]			
9.4	03/26/2024		03/26/2024	[redacted]	03/26/2024

INFORMATION SECURITY POLICY (ISP)

		[redacted]			
9.5	05/13/2024		05/13/2024	[redacted]	05/13/2024
9.6	09/30/2024		09/30/2024	[redacted]	09/30/2024

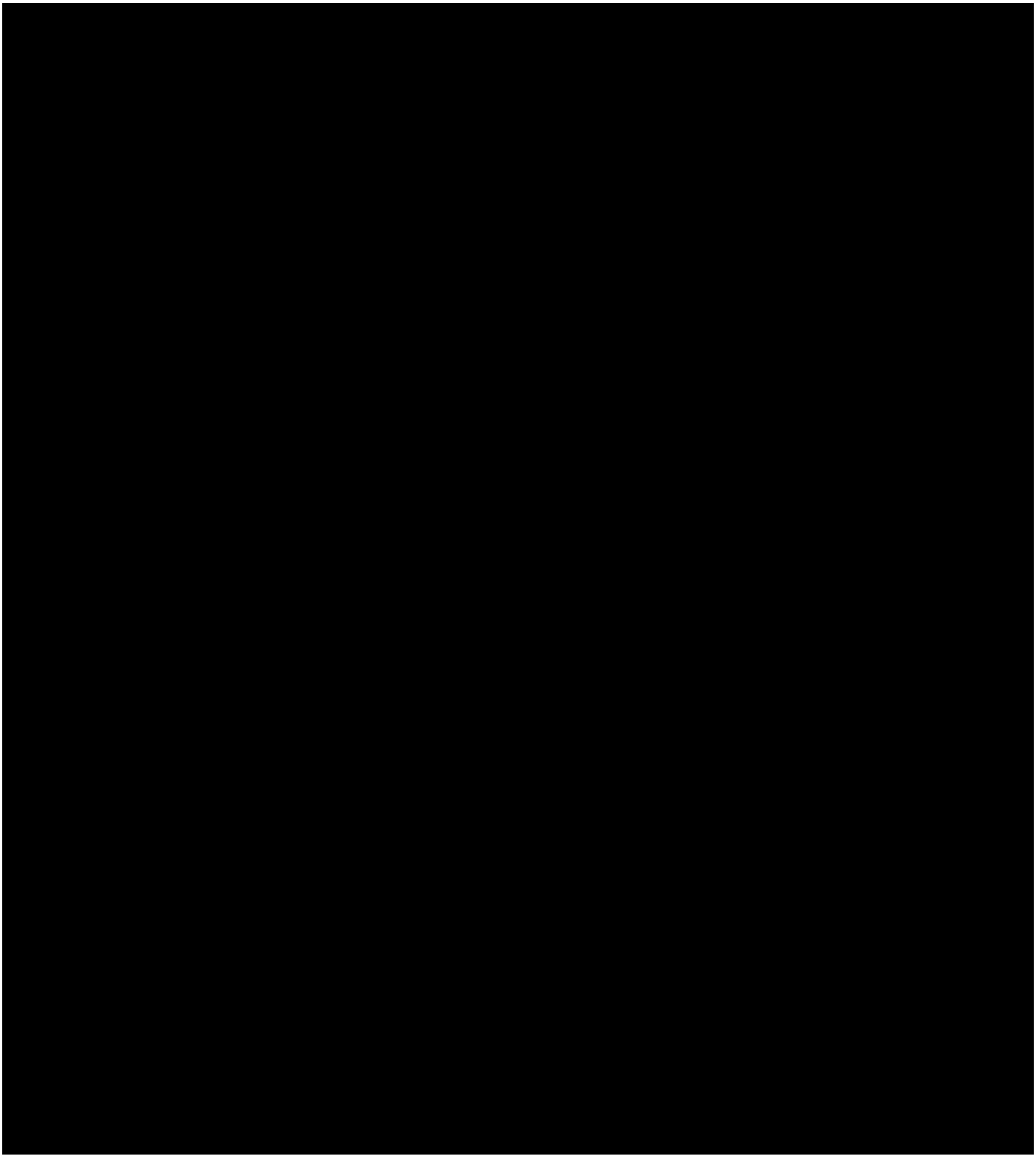
		[redacted]			
9.6.1	10/21/2024		10/21/2024	[redacted]	10/21/2024

TABLE OF CONTENTS

INFORMATION SECURITY POLICY (ISP)

1 Section I: Overview of Information Security

1.1 Introduction



[redacted]

1.2 Rules of Behavior for Users and Managers of Information Resources

[redacted]

1.2.1 Management Responsibilities

[redacted]

1.2.2 User Responsibilities

1.2.2.1 Accountability

[redacted]

1.2.2.2 Integrity

[redacted]

1.2.2.3 Confidentiality

[redacted]

1.2.2.4 Awareness and Training

[redacted]

[redacted]

1.2.2.5 Sensitive Information

[redacted]

1.2.2.6 Hardware, Software, and Copyright Protection and Control

[redacted]

1.2.2.7 Alternative Worksite (Non-SSA Controlled Locations)

[redacted]