



EQUIFAX®

Security Incident Handling Procedure Guide

July 2017
Version 9.6

Based on NIST Special Publication 800-61, Computer Security Incident Handling Guide, this manual establishes procedures for handling Security incidents that may compromise the availability, integrity and confidentiality of Equifax data and resources.

Document Change Management

Document Name	Security Incident Handling Procedure Guide		
Type:	Policy & Procedures	Equifax Policy No.	
Policy Owner:	Berlene Herren	Issued By:	Global Security
Approved By:	Stephen Cosby, Susan Mauldin	Prepared By:	Amanda Le
Effective Date:	June 2007		
Last Reviewed Date:	July 2017	Next Review Date:	July 2018

VERSION CONTROL

Date	Name	Version	Description of Changes
May 2006	Nick Nedostup	1	Production document created.
June 2008	N. Nedostup, D. Amster, S. Choffery	6	Updated to combine Technical, Data and Physical Security Plans into one unified Security Incident Response Plan.
February 2009	N. Nedostup, D. Amster, S. Choffery	7	Yearly Updates
February 2010	N. Nedostup, D. Amster, S. Choffery	8	Yearly Updates
February 2011	N. Nedostup, D. Amster, S. Choffery	9	Yearly Updates
October 2011	N. Nedostup, D. Amster, S. Choffery	9.1	Updated to reflect organizational/employee changes. Added Document Change Management Section.
November 2011	N. Nedostup	9.1	Updated Section 3.1 to include frequency of IR Contact List review & updates.
March 2012	Ray Strubinger	9.1.2	Updated Appendix F and created a separate document for the information. Verified web addresses. Minor corrections to wording and terminology.
October 2012	Ray Strubinger	9.3	Update to DDoS procedure
June 2014	Francis Finley	9.4	Update to correct grammar, formatting, clarify language, and organization restructuring
October 2014	Francis Finley	9.5	Update to fix section on Forensics/Malware handling, include additional contacts, Archer ticketing information.
October 2014	Ted Mac Daibhidh, CD	9.5.1	Standardized formatting throughout document; corrected various errors; restructured lists to be easier to reference/read, resized figures to be more readable; changed heading font and colors to match official template document; corrected "single point lists"; updated ToC.
October 2015	Susan Mauldin	9.5.1	Reviewed with no revisions
October 2016	Susan Mauldin	9.5.1	Reviewed with no revisions
July 2017	Morphick, Francis Finley, Berlene Herren, Amanda Le, Michael Douglas, Stephen Cosby, Bryce Williams	9.6	General cleanup, Added CAT Triage, IR best practices, and Kill Chain model, document name change from "Security Incident Handling Policy & Procedure Guide" to "Security Incident Handling Procedure Guide"

Table of Contents

Document Change Management 2

1. General Information 4

 1.1 Purpose 4

 1.2 Goal 4

 1.3 Scope 4

 1.4 Reporting a Suspected Incident 5

 1.5 Roles and Responsibilities 5

2. SIRT Activation and Initiation Process 8

 2.1 Overview 8

 2.2 Incident Response Management Bridge Procedure 8

3. Incident Handling Guidelines 10

 3.1 Overview 10

 3.2 Goals & Priorities 10

 3.3 Incident Definition and Declaration 10

 3.4 Incident Classification 11

 3.5 Crisis Management Trigger Framework 12

 3.6 Overview 12

 3.7 Trigger Checklist 12

4. Incident Response Phases 13

 4.1 Overview 13

 4.2 Detection and Analysis 14

 4.3 Containment, Eradication and Recovery 15

 4.4 Post-Incident Activity 15

 4.5 Incident Report Handling Guidelines 16

5. Cyber Investigation Procedures 17

 5.1 Denial of Service or Distributed Denial of Service (DoS or DDos) 17

 5.2 Malicious Code Incident Handling 17

 5.3 Unauthorized Access Incident Handling 17

 5.4 Inappropriate Usage Incident 18

 5.5 Phishing Response Procedures 18

 5.6 Vulnerability Management Procedures 18

 5.7 Evidence Handling and Shipping Procedures 19

 5.8 Remote Imaging Procedures 19

6. Fraud Investigation and Monitoring Procedures 19

7. Physical Security Event Procedures 19

 7.1 Overview 19

 7.2 General Procedures 19

 7.3 Lost/Stolen Asset Investigation Procedures 20

 7.4 Life Safety Incident Commander Responsibilities 20

 7.5 Fire Procedure 20

 7.6 Tornado Procedure 20

 7.7 Bomb Procedure 20

 7.8 Medical Emergency Procedure 21

8. Security Event Consumer Notification Procedures 21

 8.1 Consumer Notification Procedures 21

 8.2 Law Enforcement Notification 22

Appendix A - Definitions 23

Appendix B - Abbreviations 25

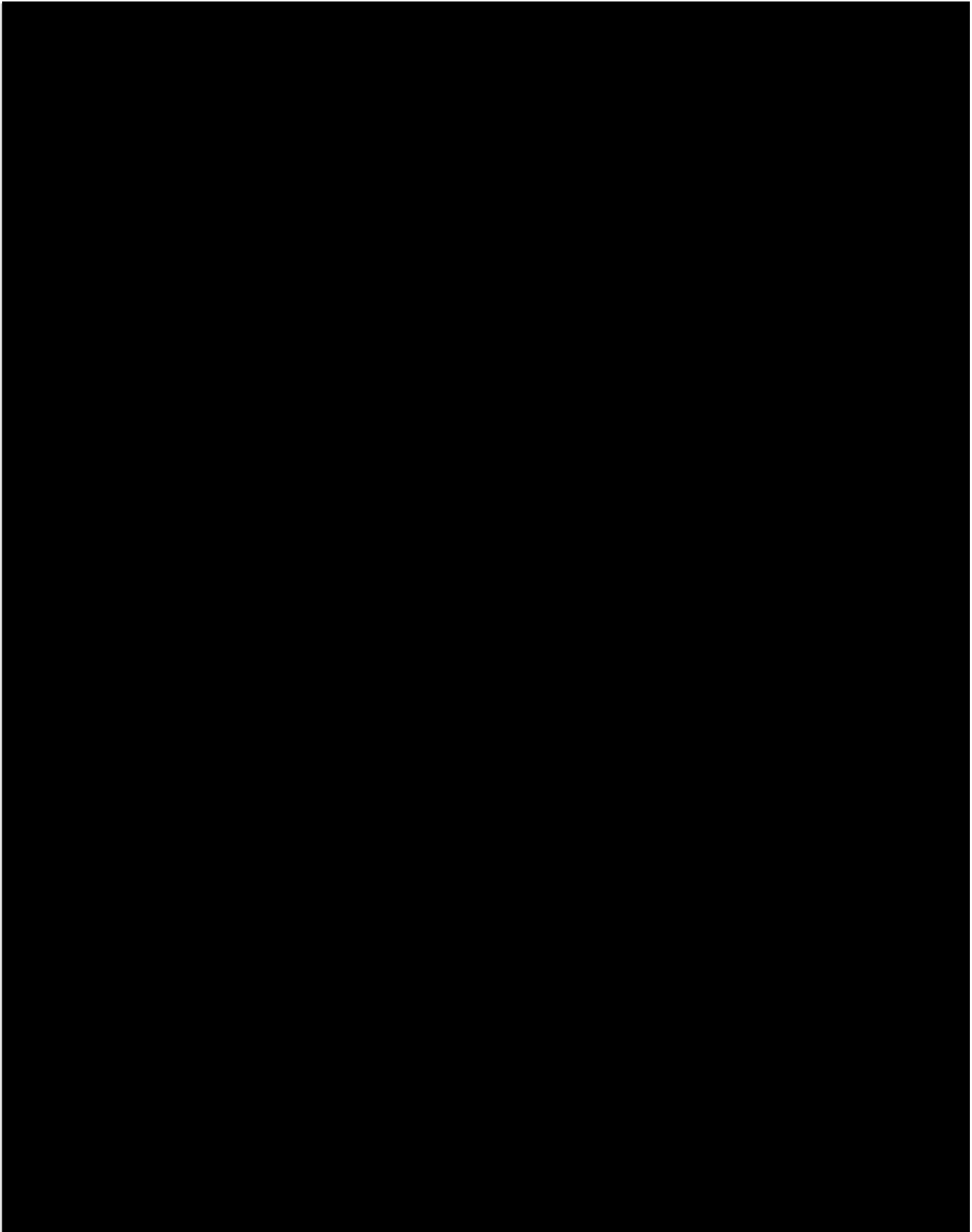
Appendix C - Incident Classification Matrix 26

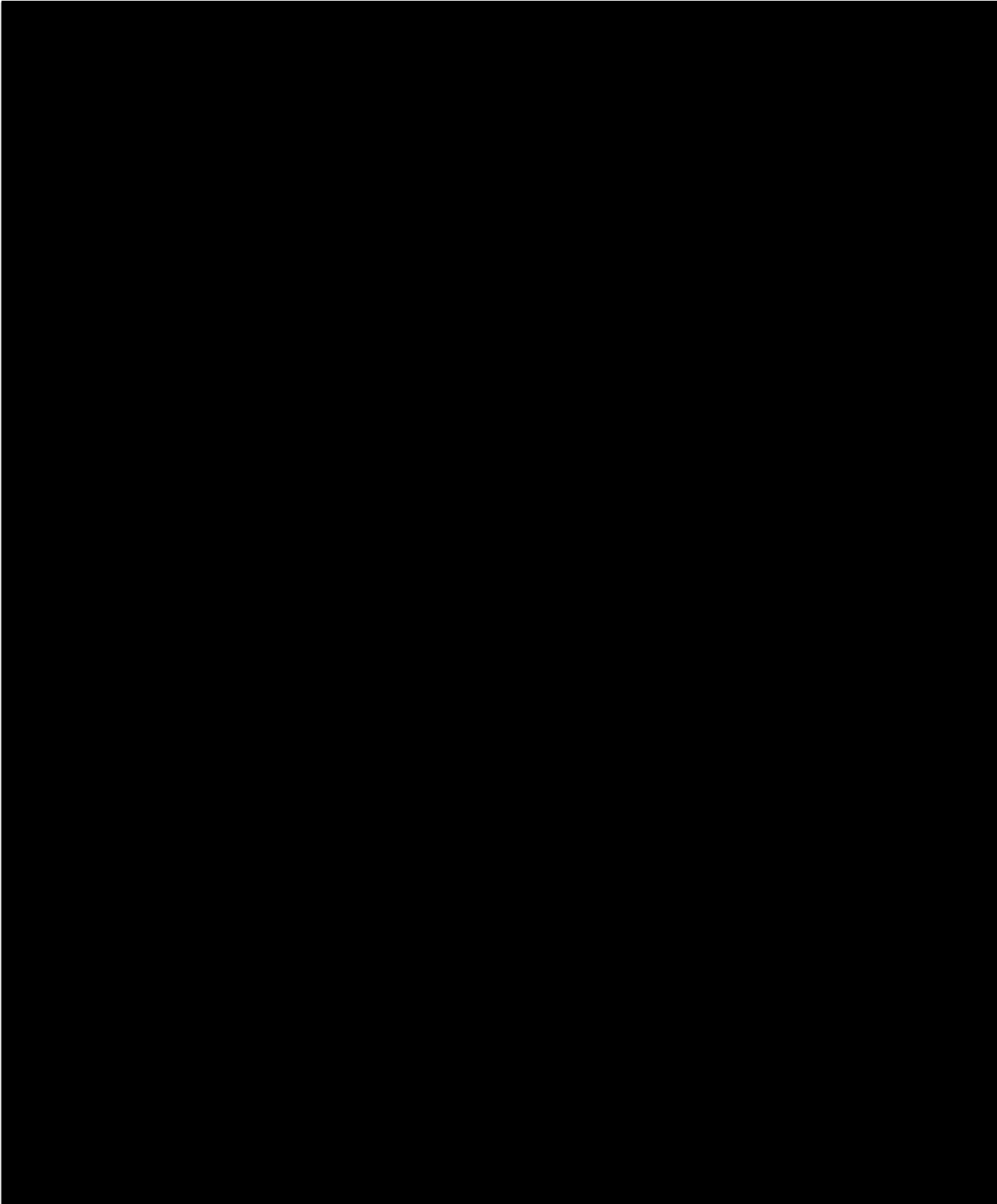
Appendix D - Archer Ticketing System 27

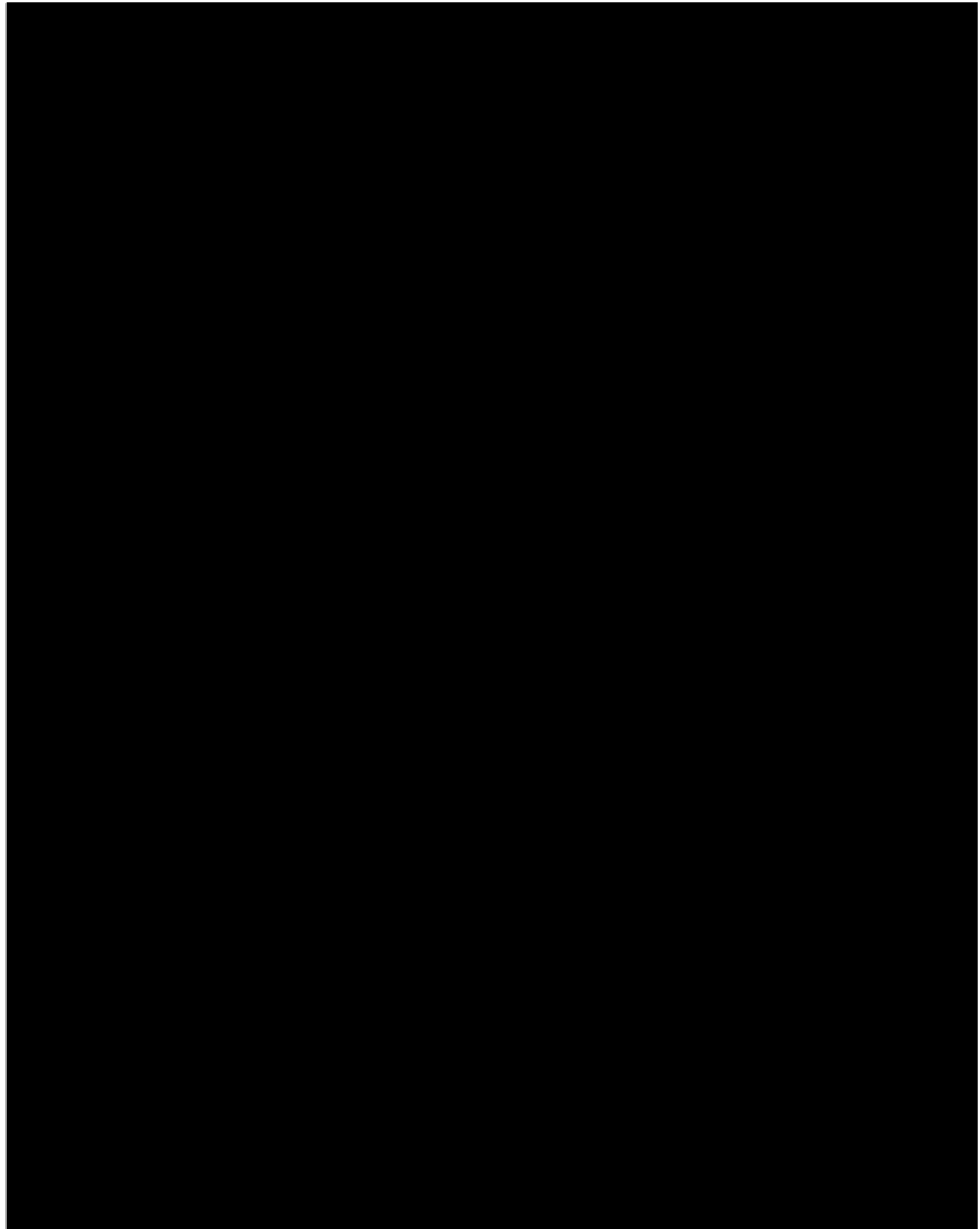
Appendix E - Physical Security Emergency Contacts 28

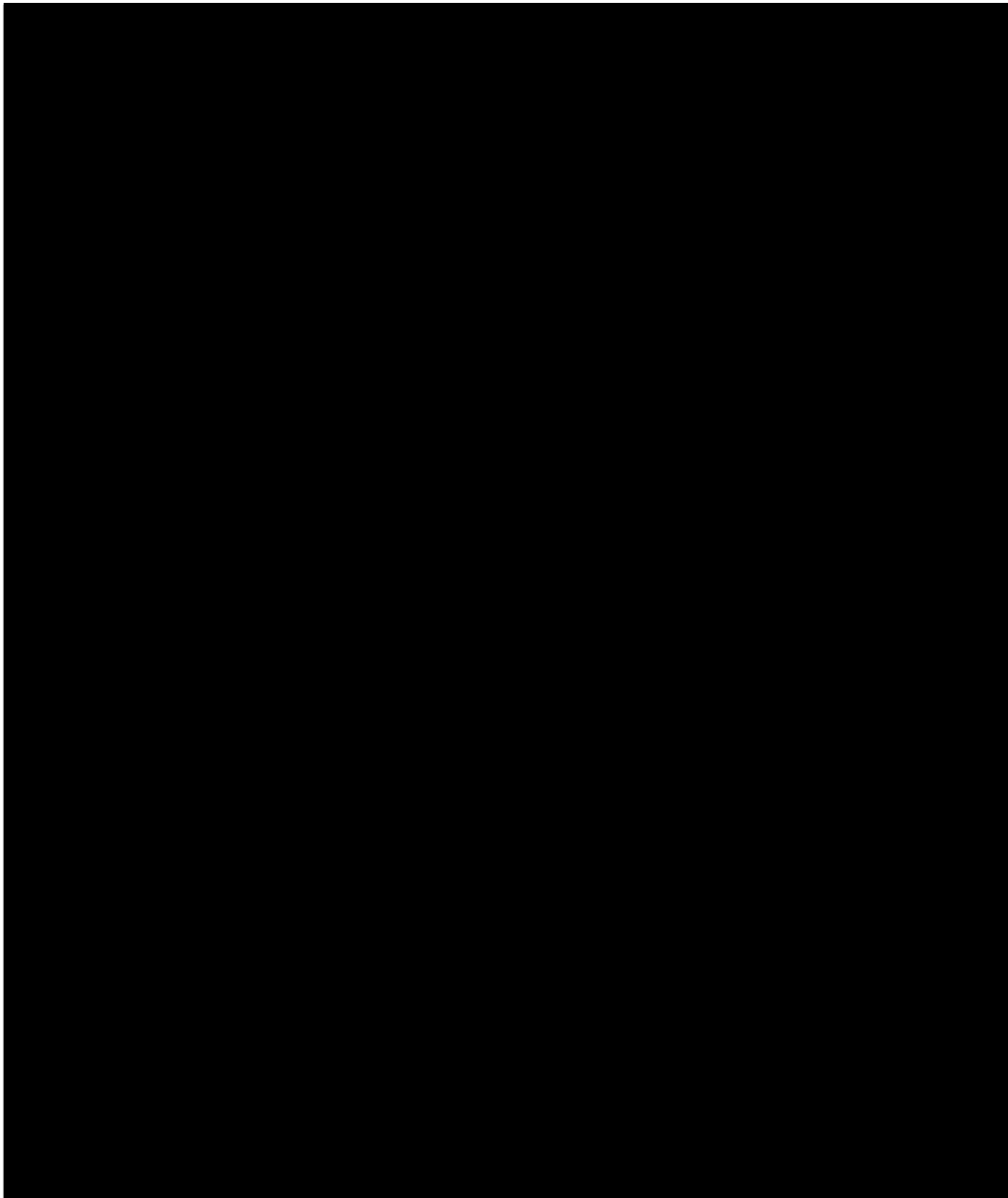
Appendix F - Payment Card Industry (PCI) and Contract Contact References 29

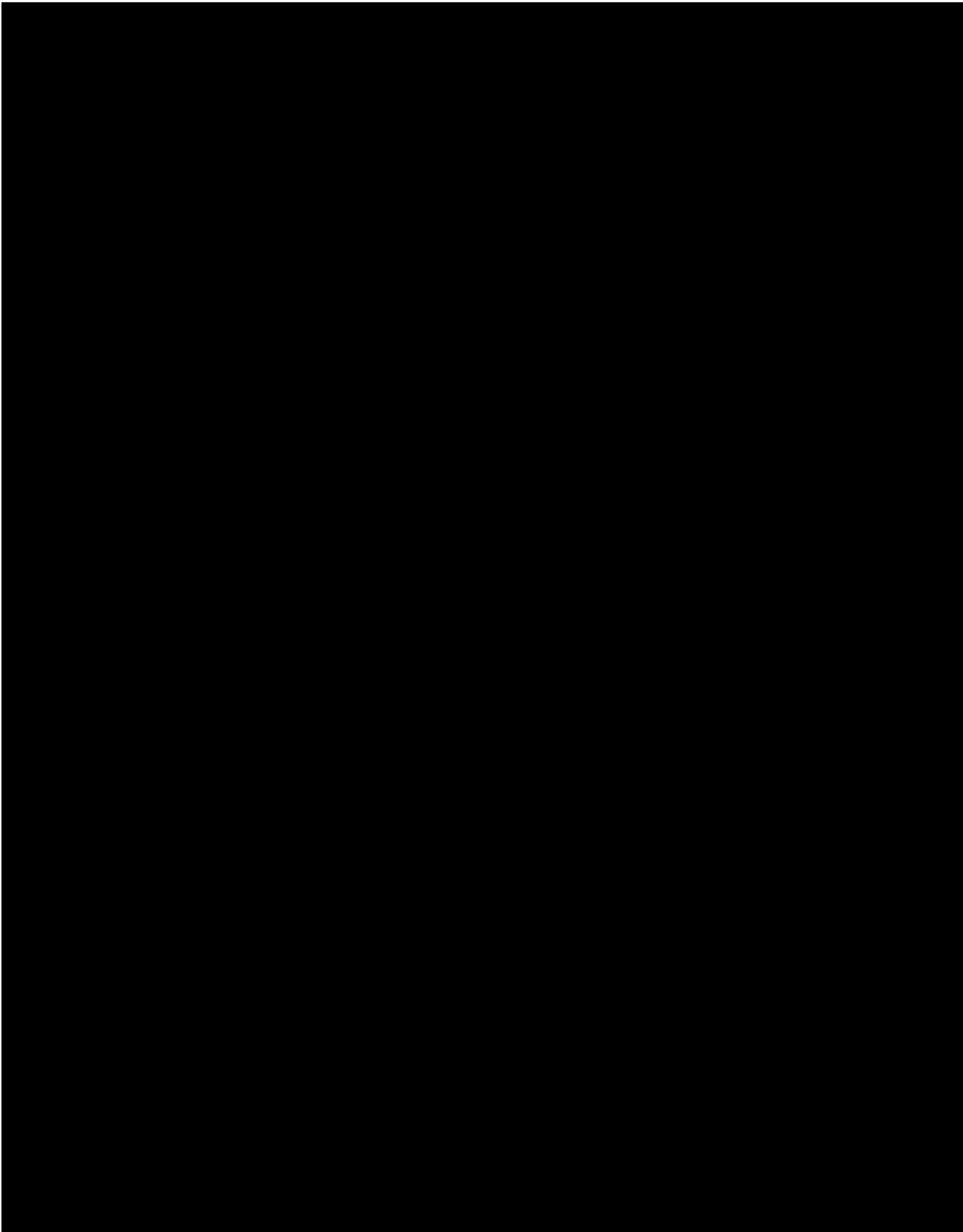
Acknowledgements 30

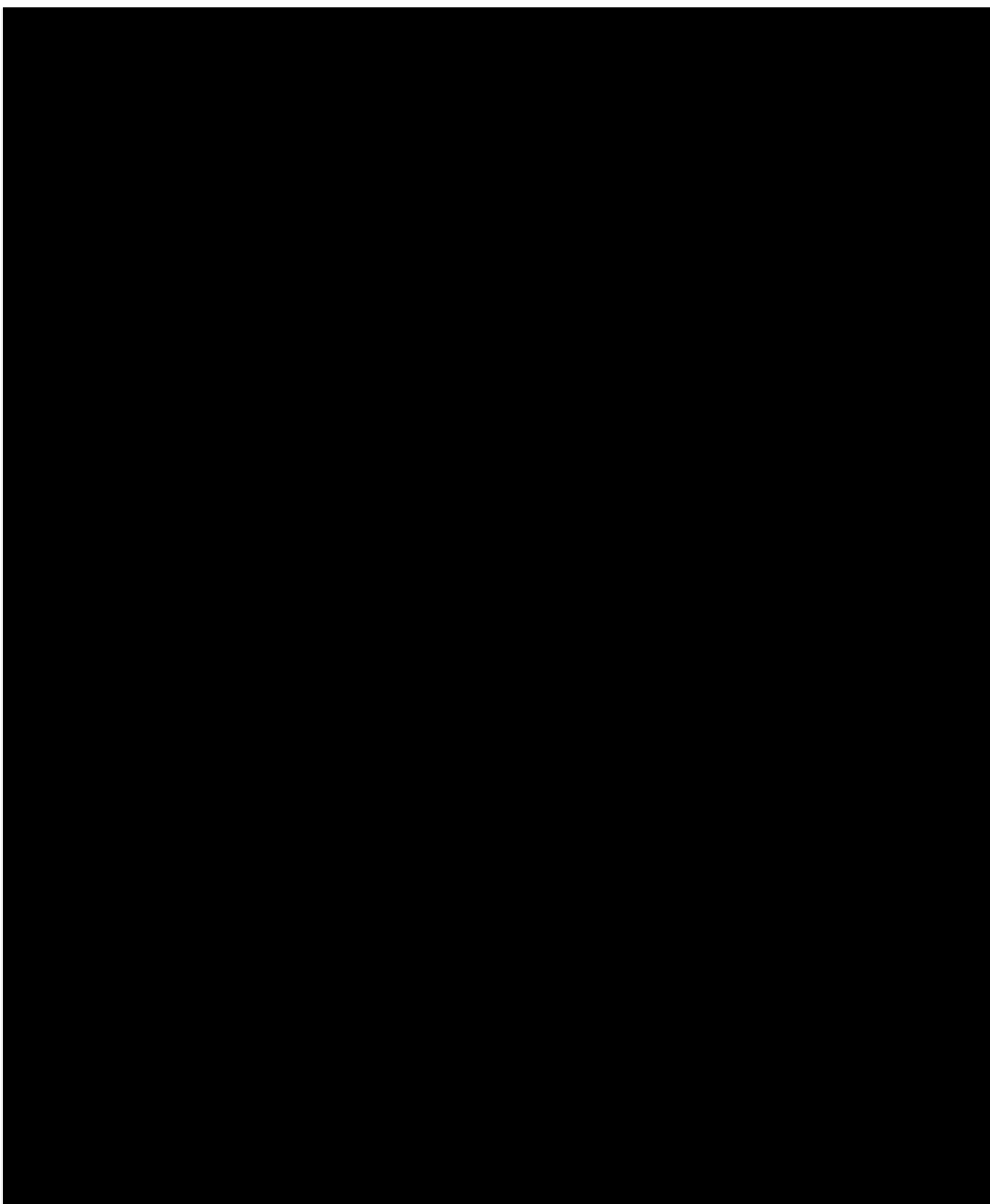


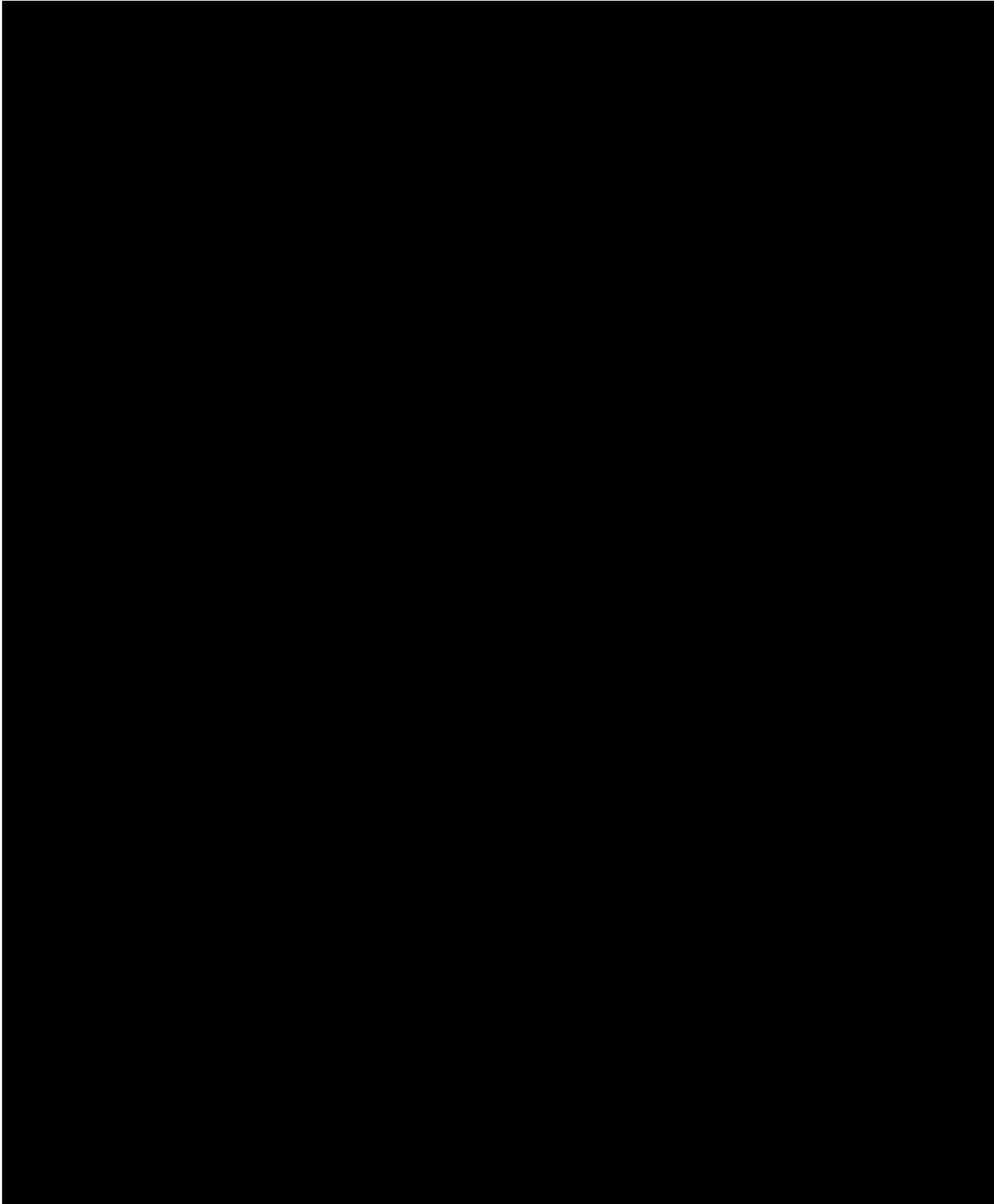


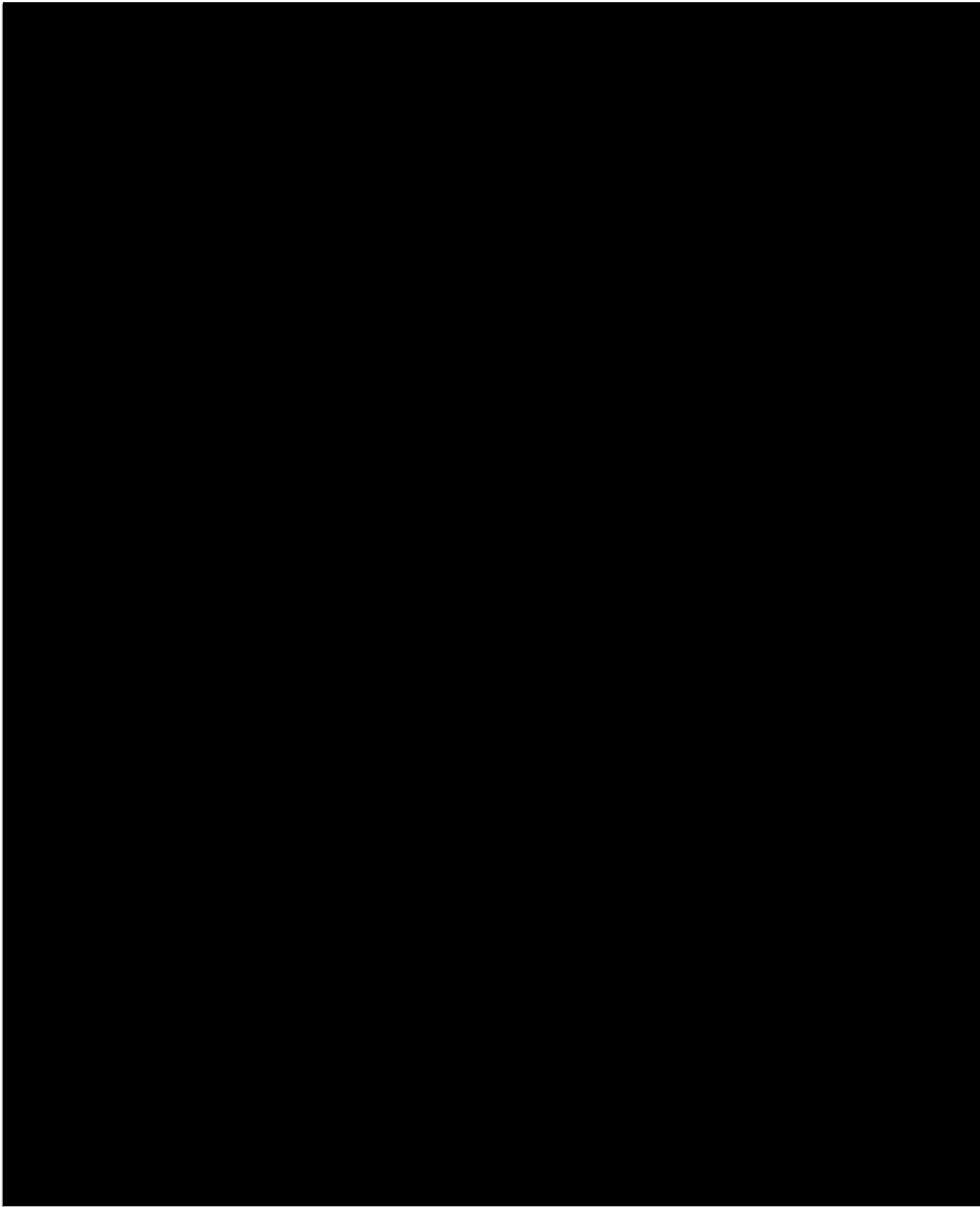


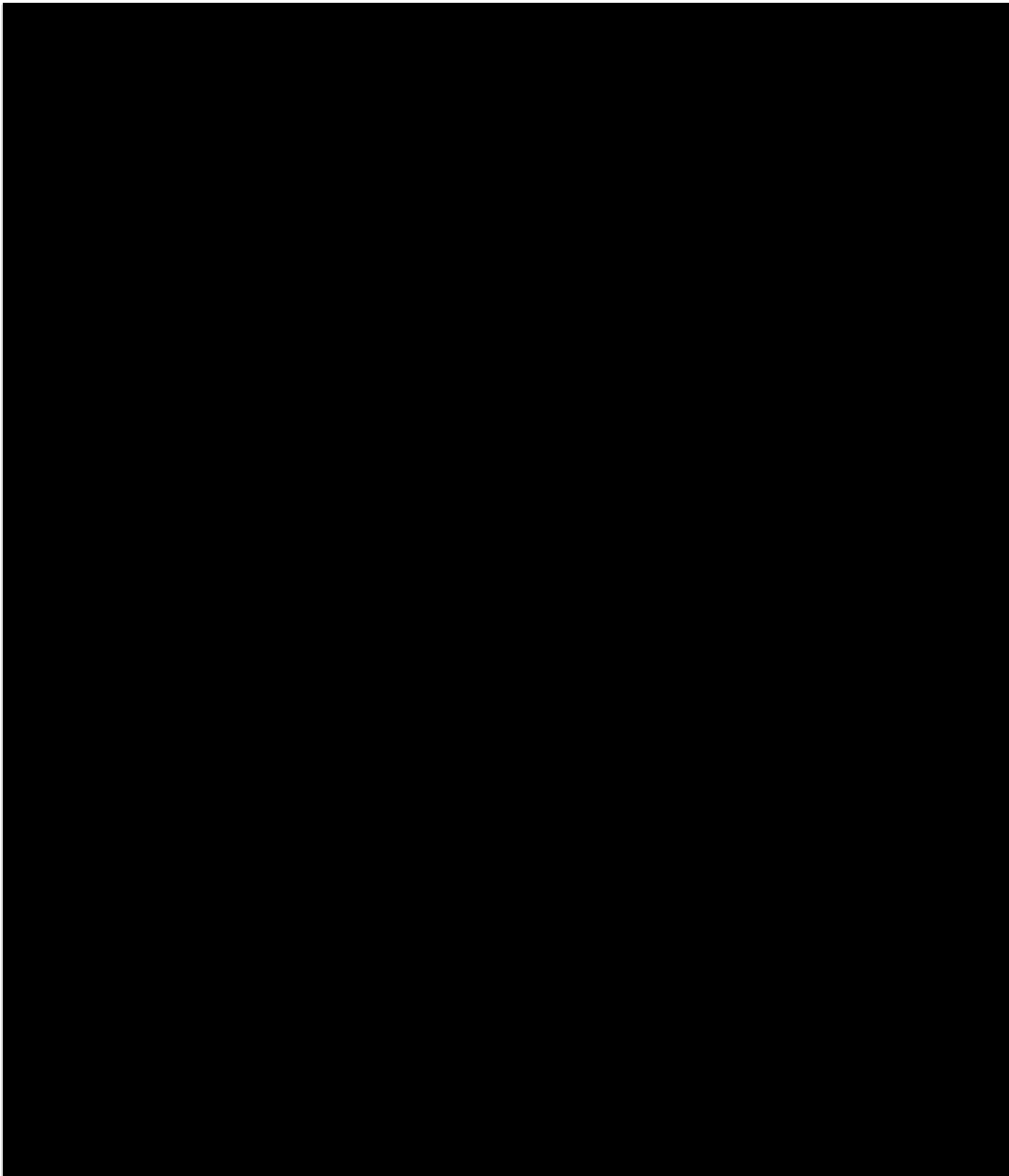


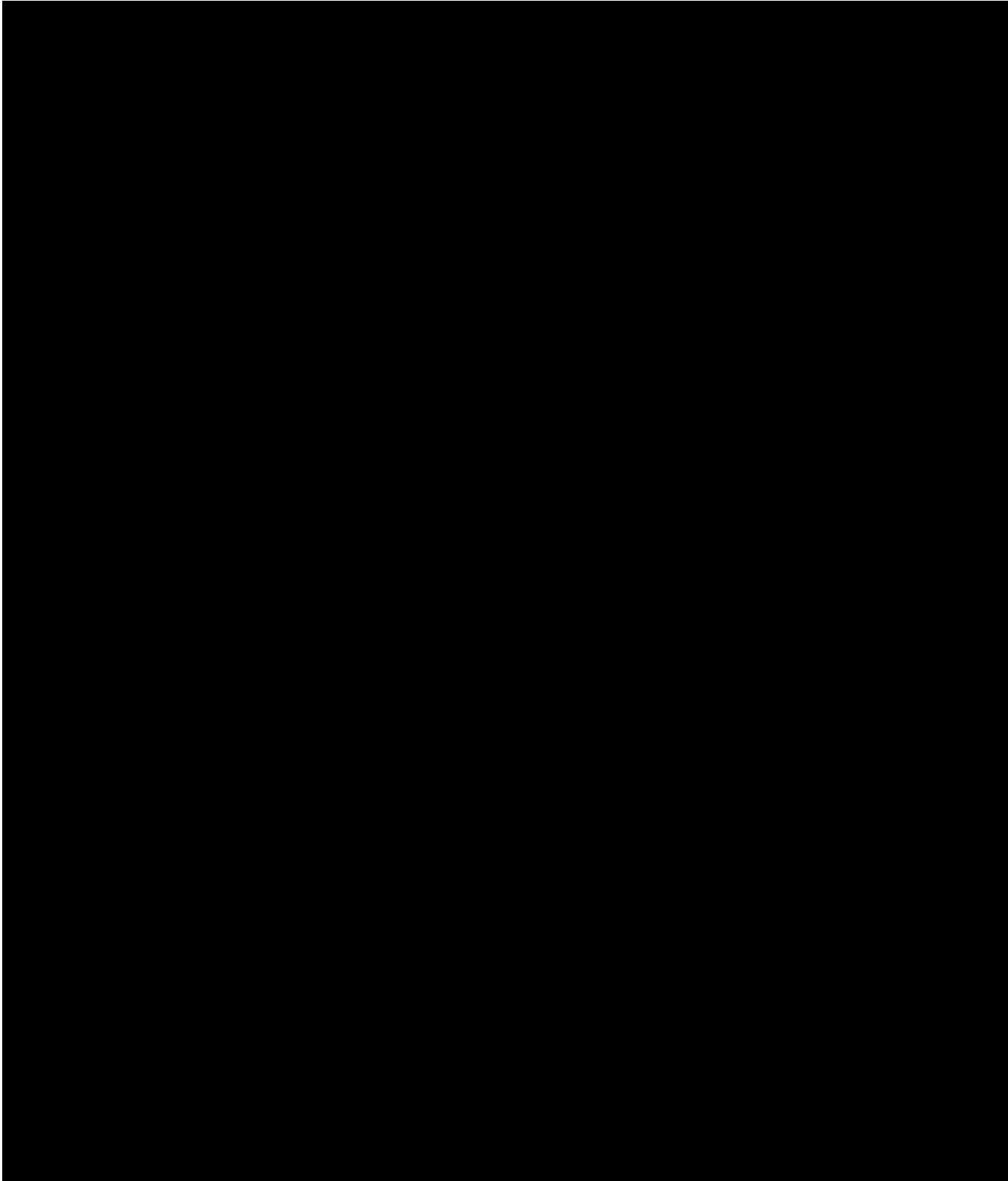


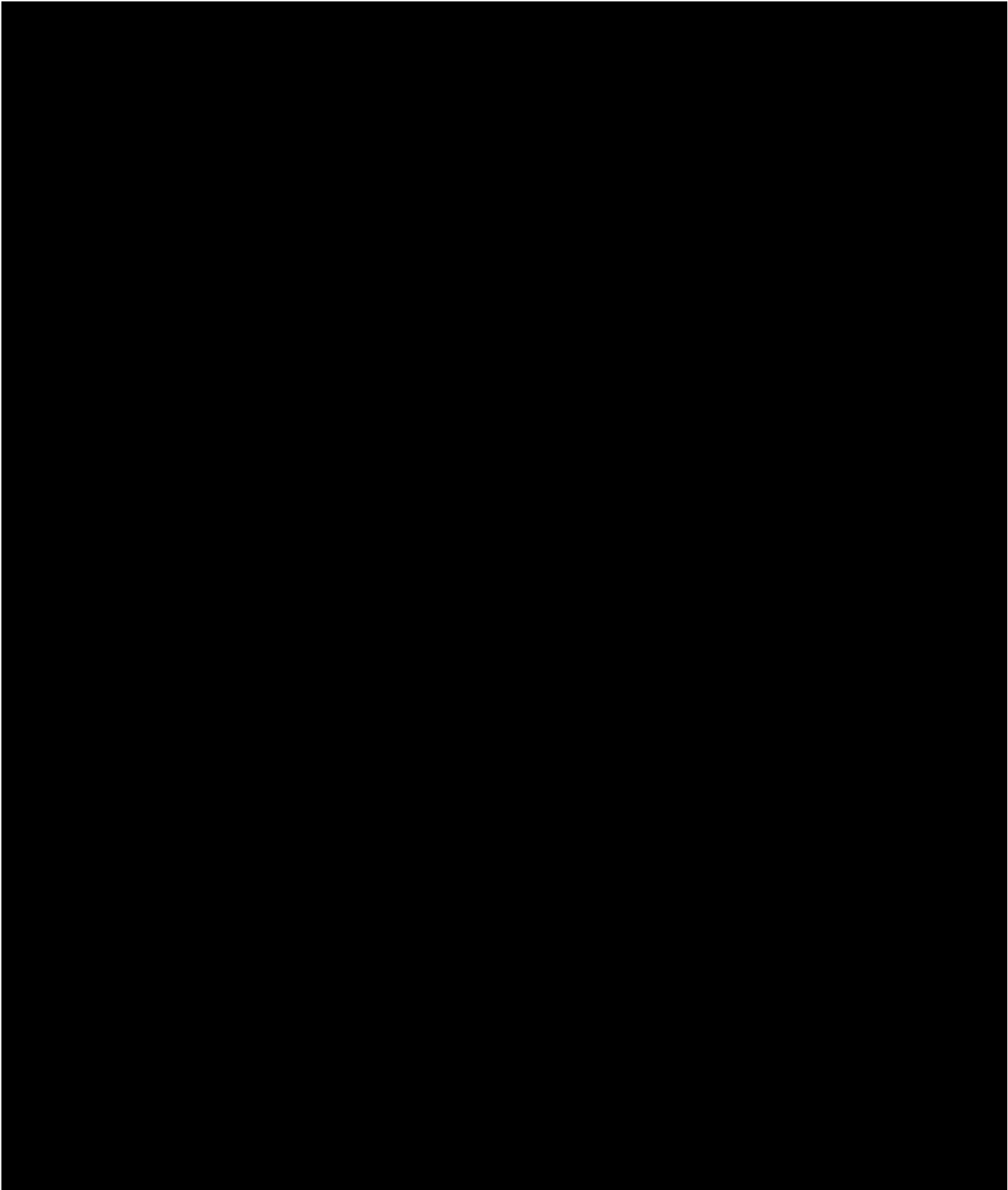


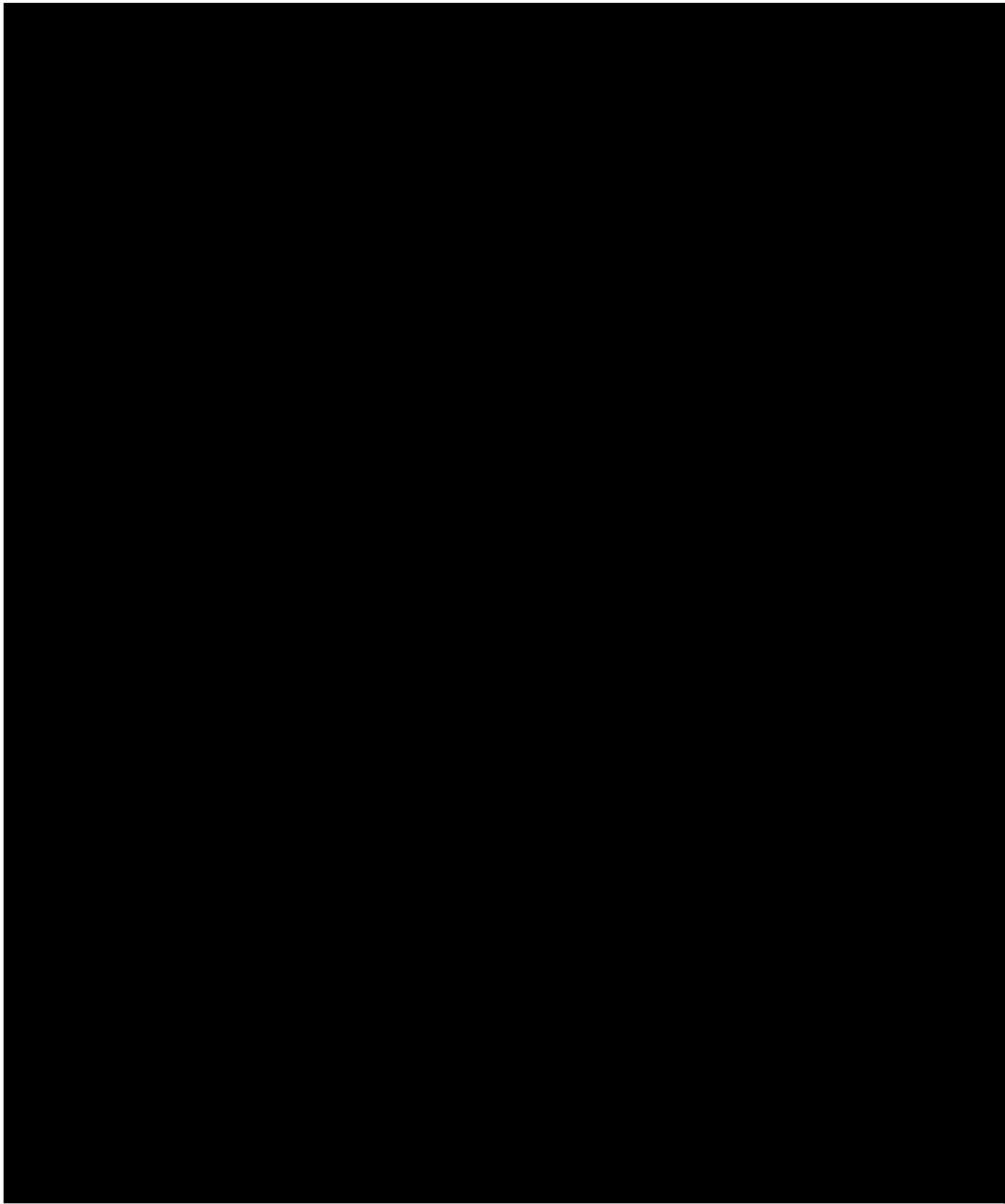


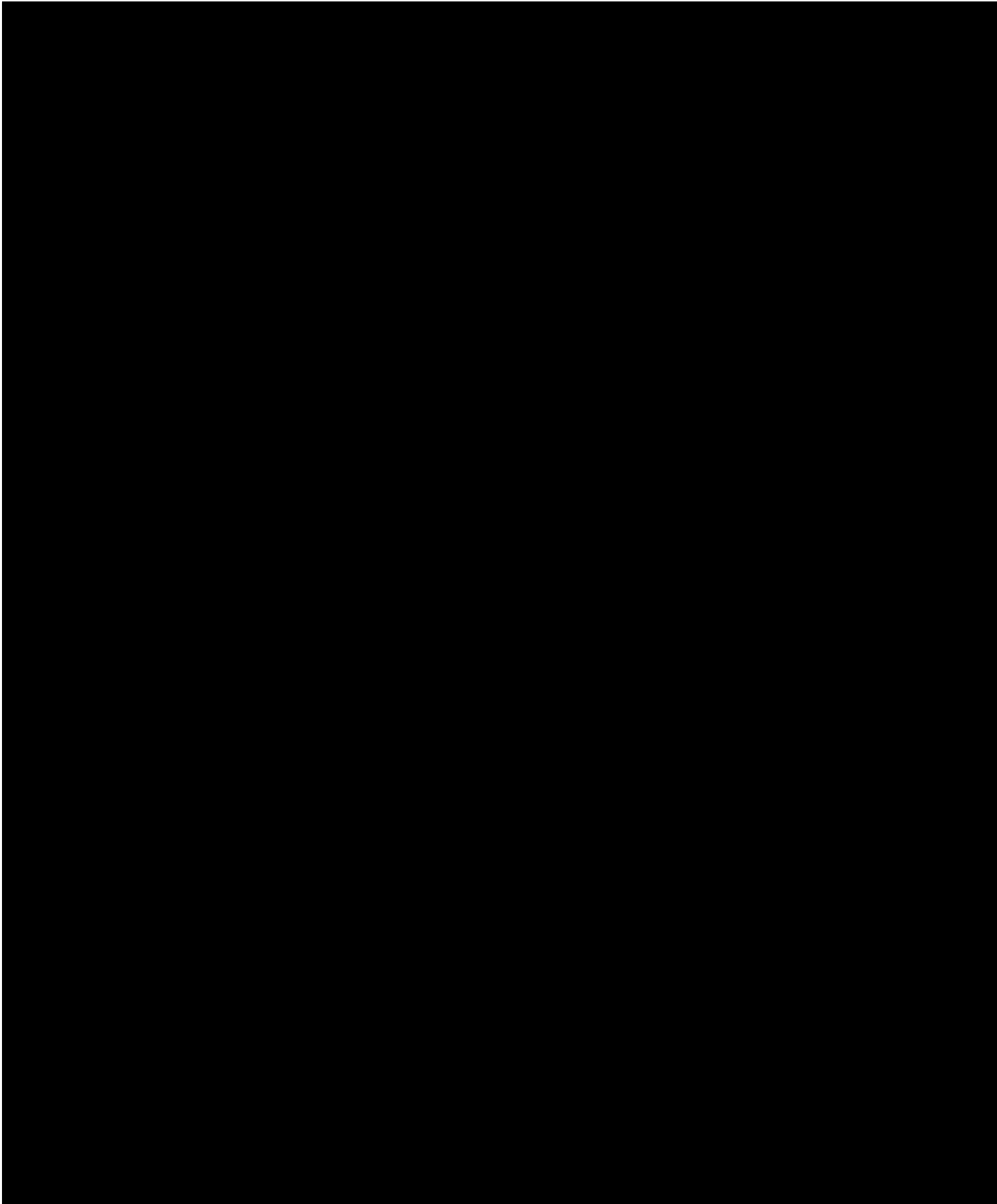


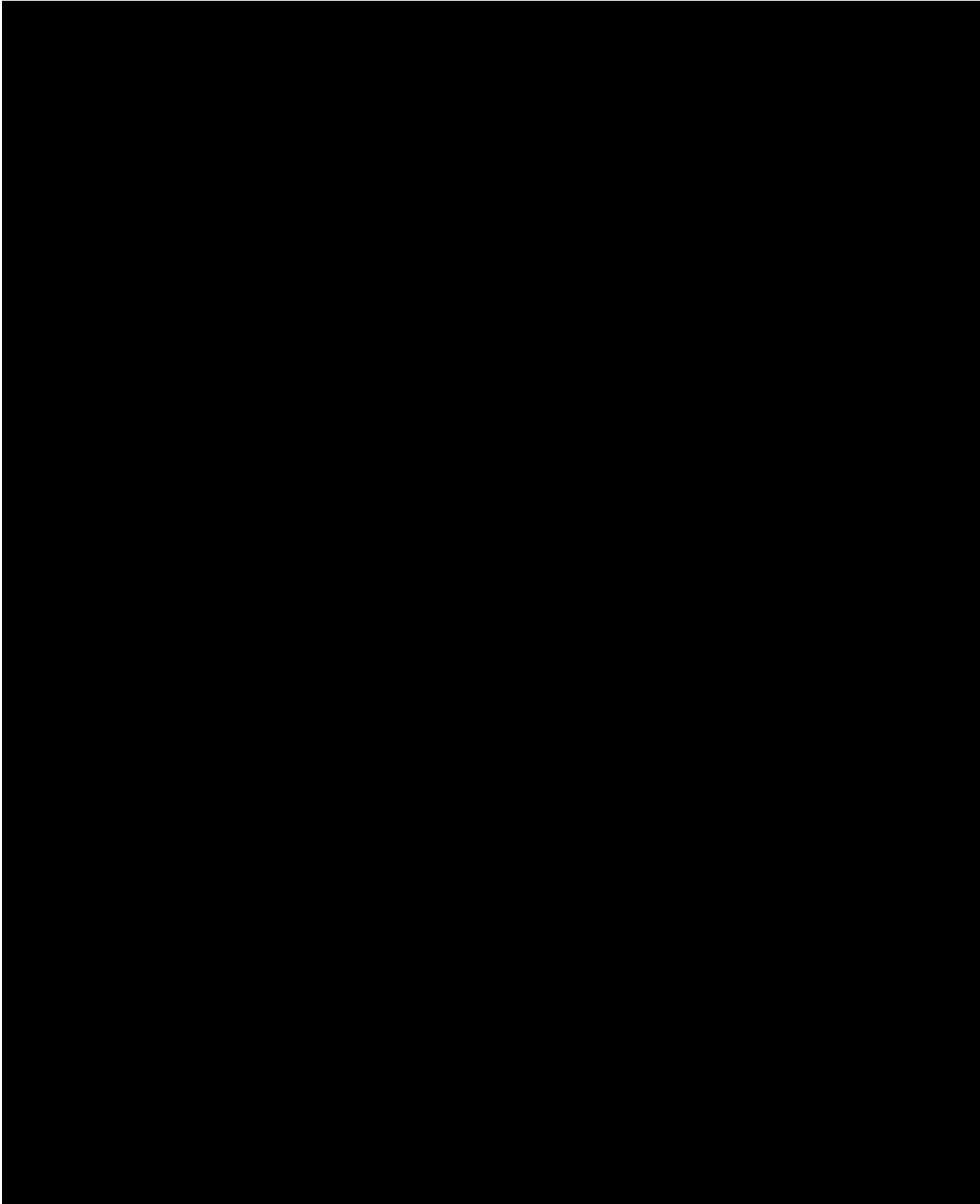


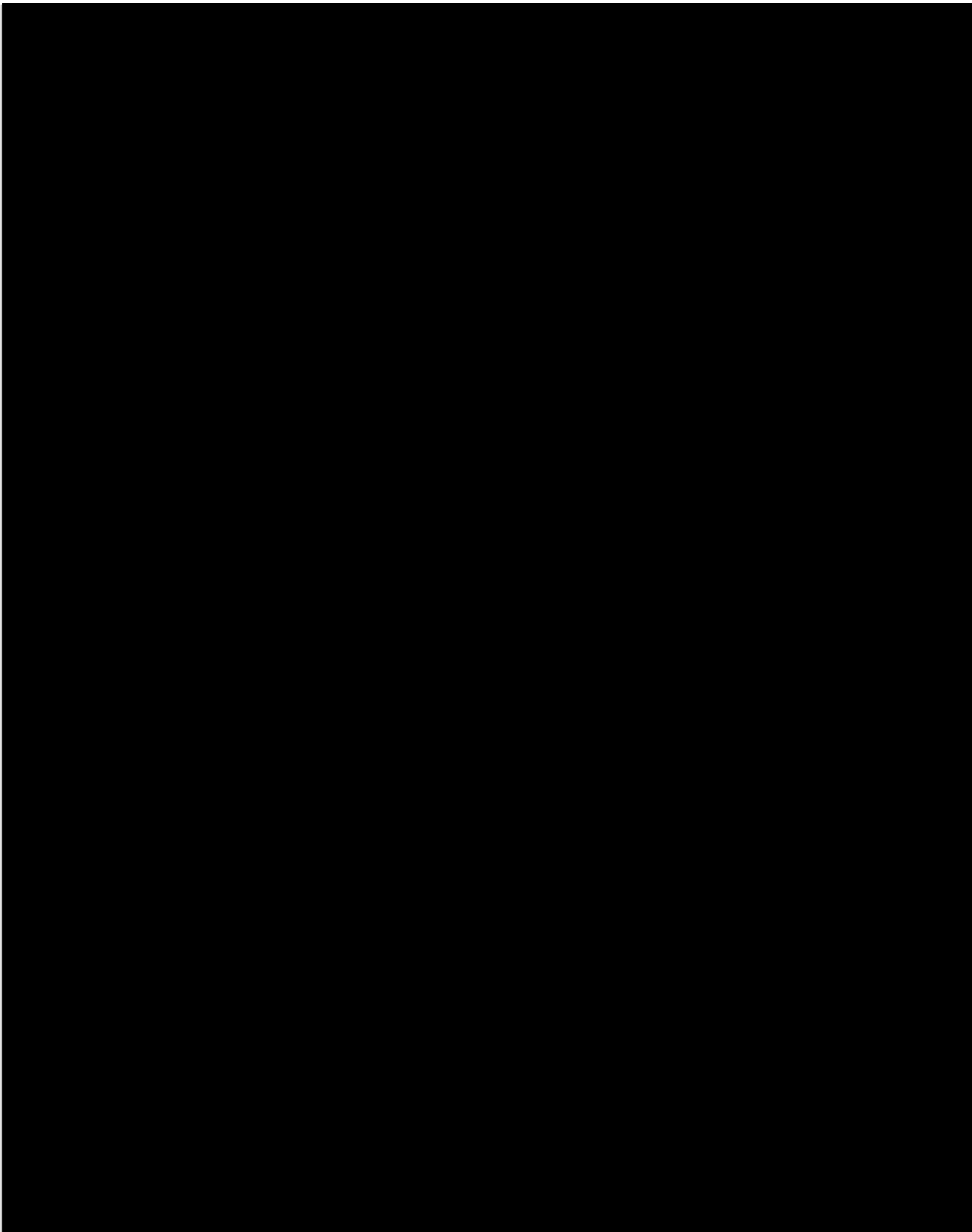


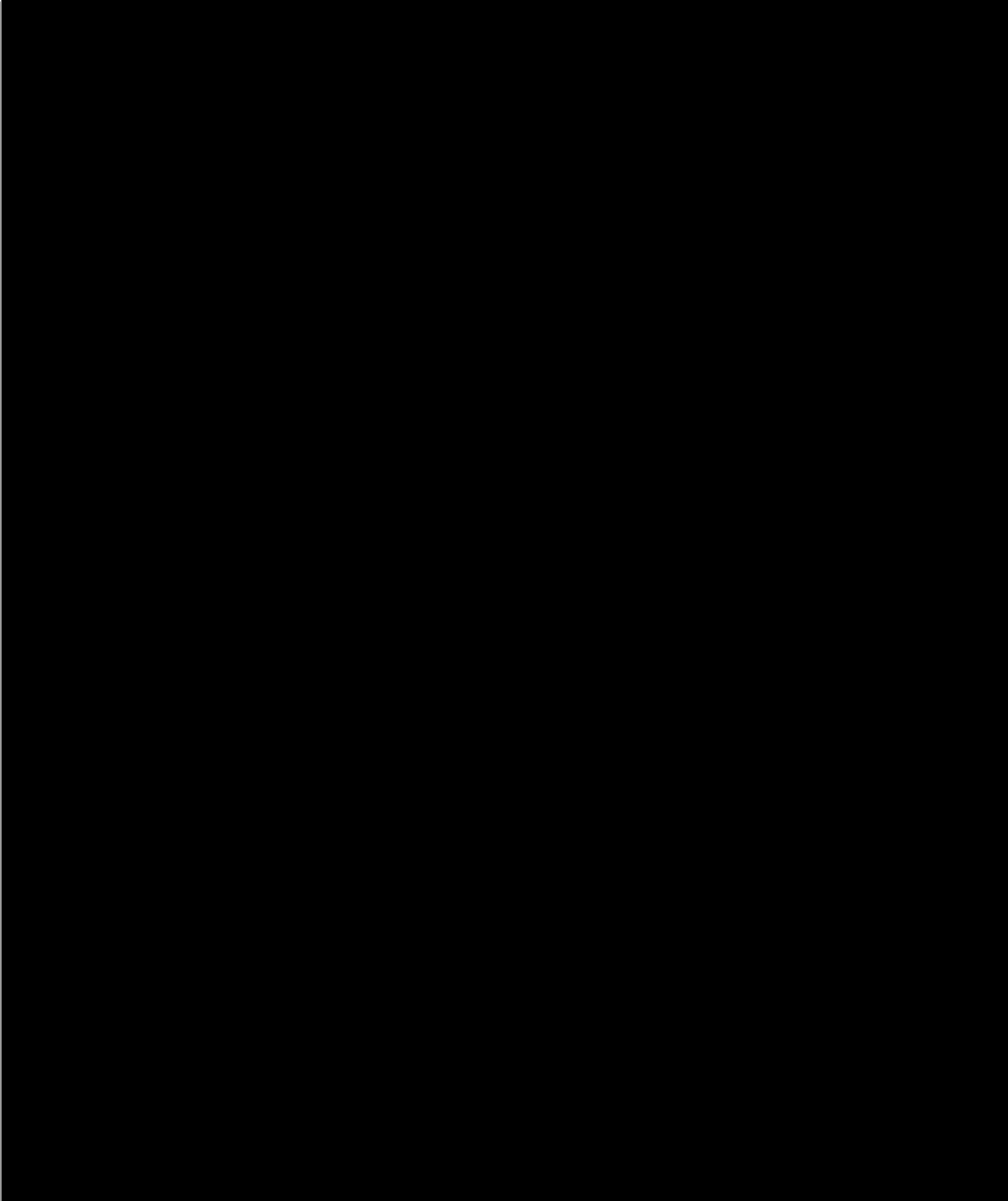


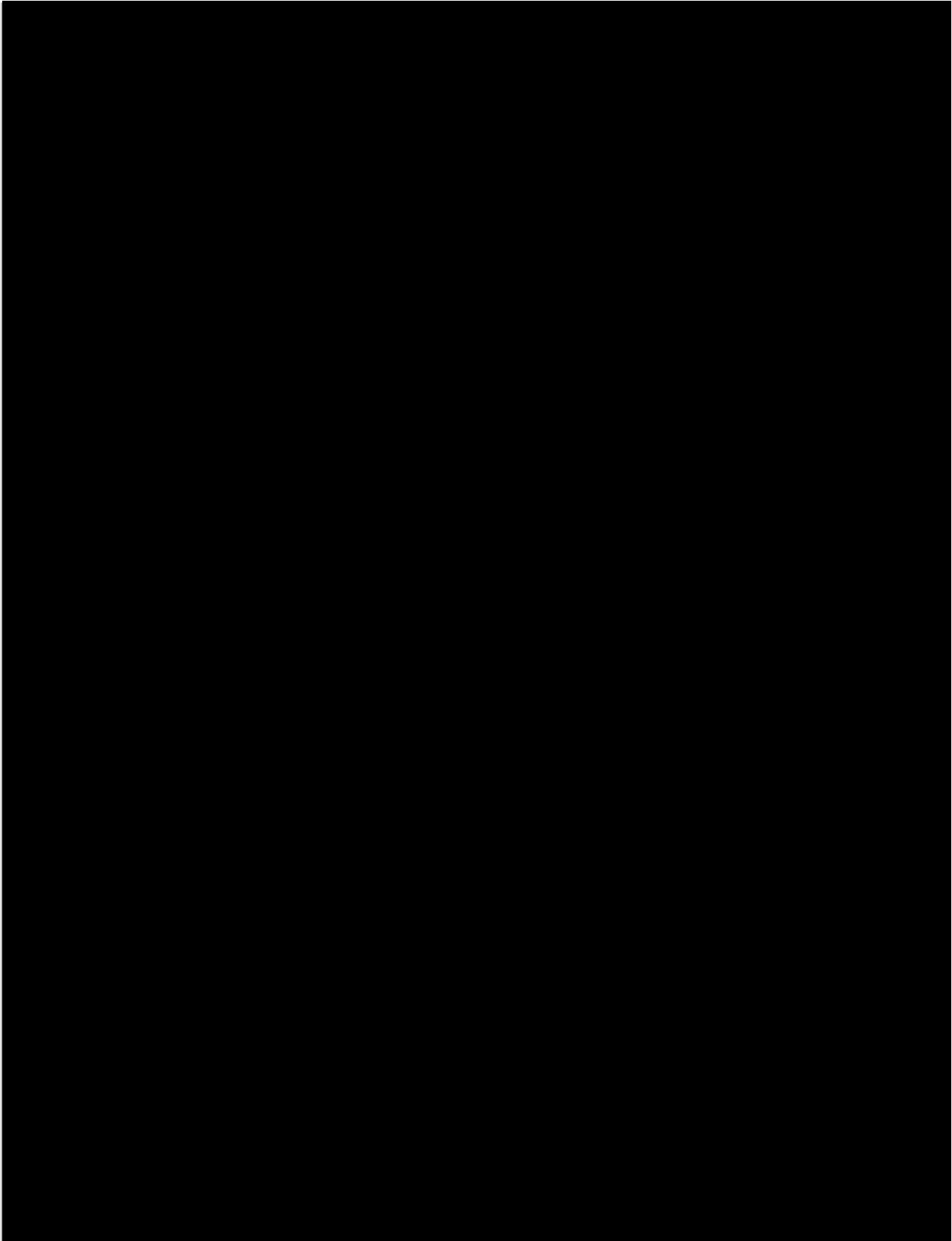


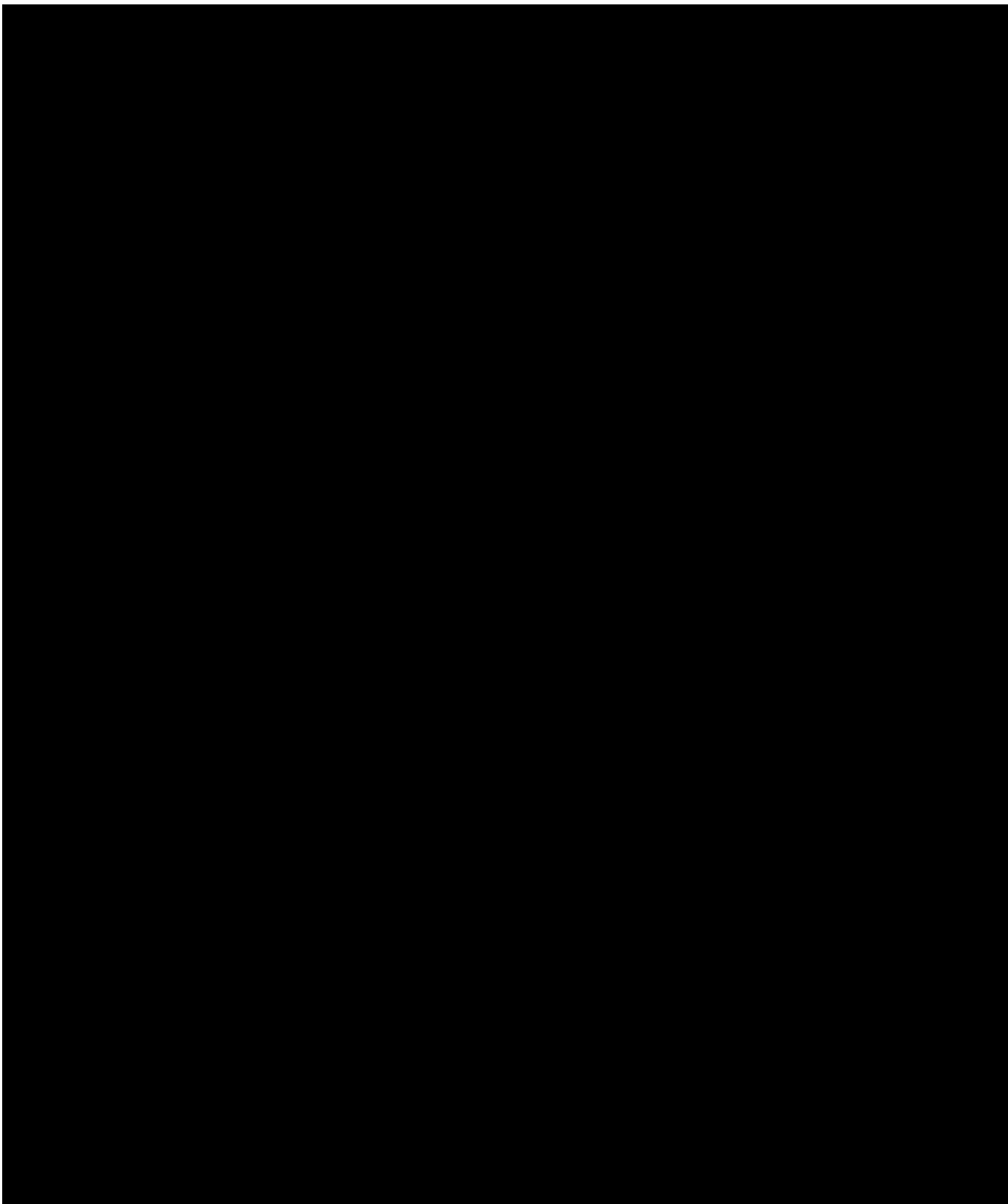


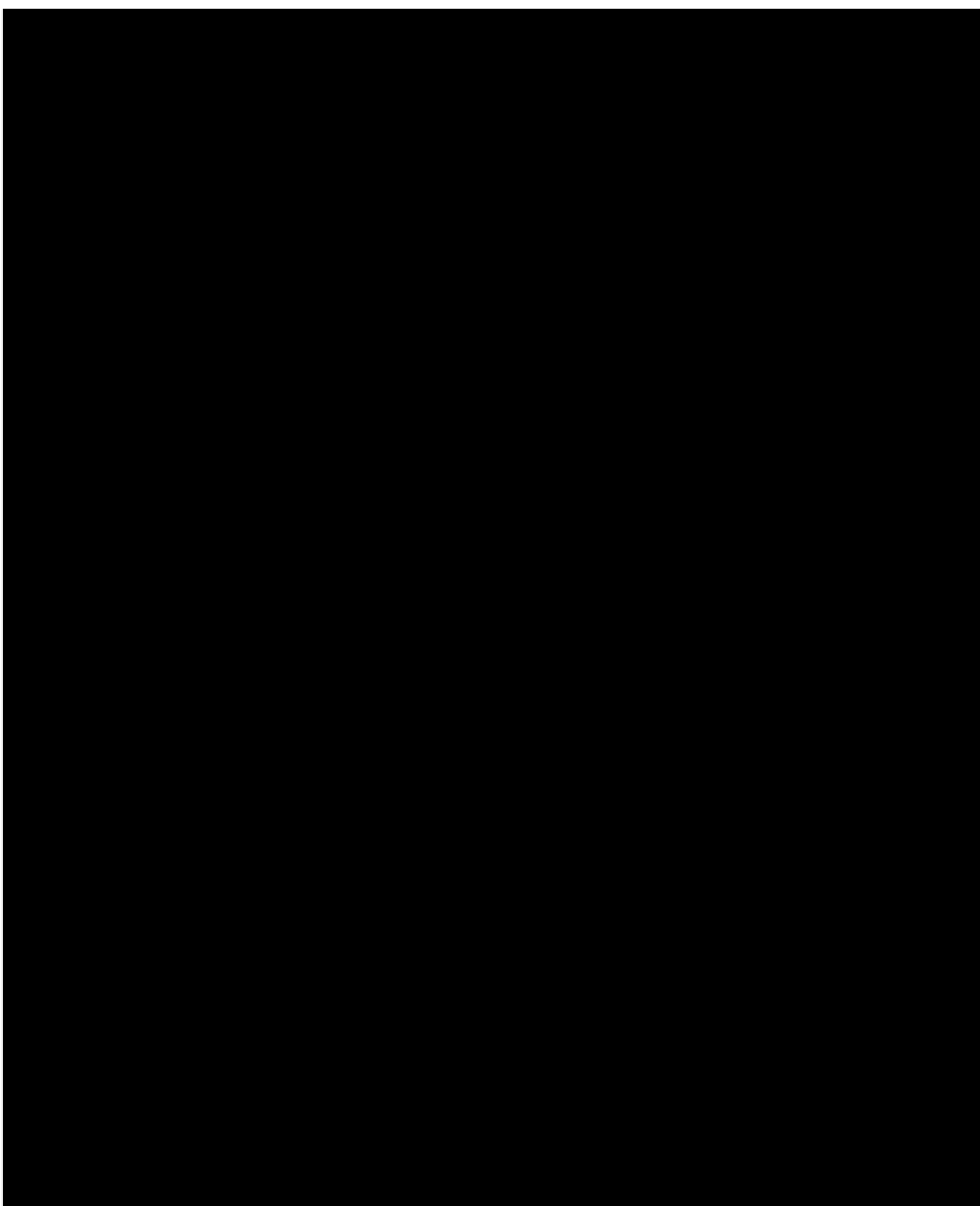


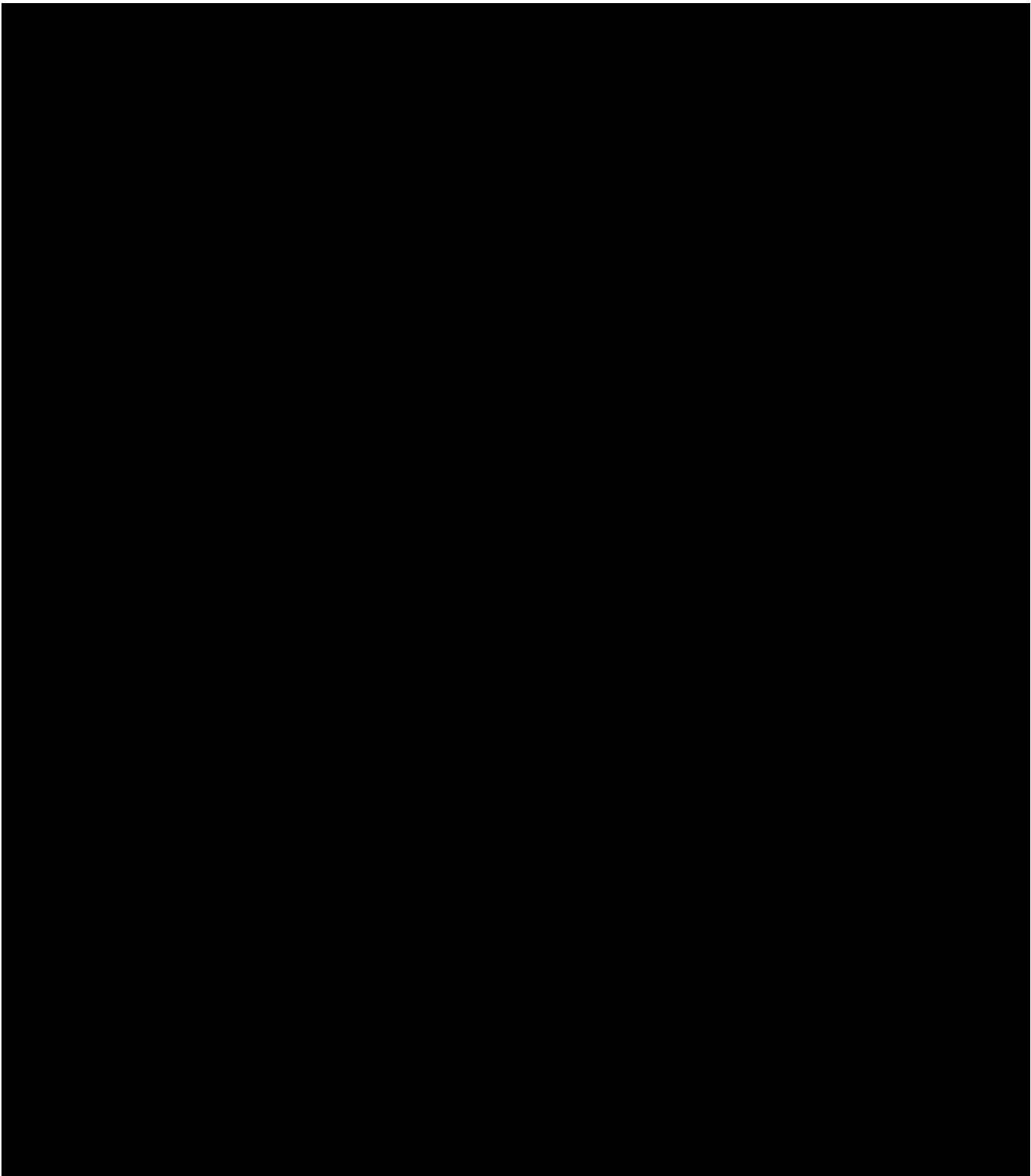


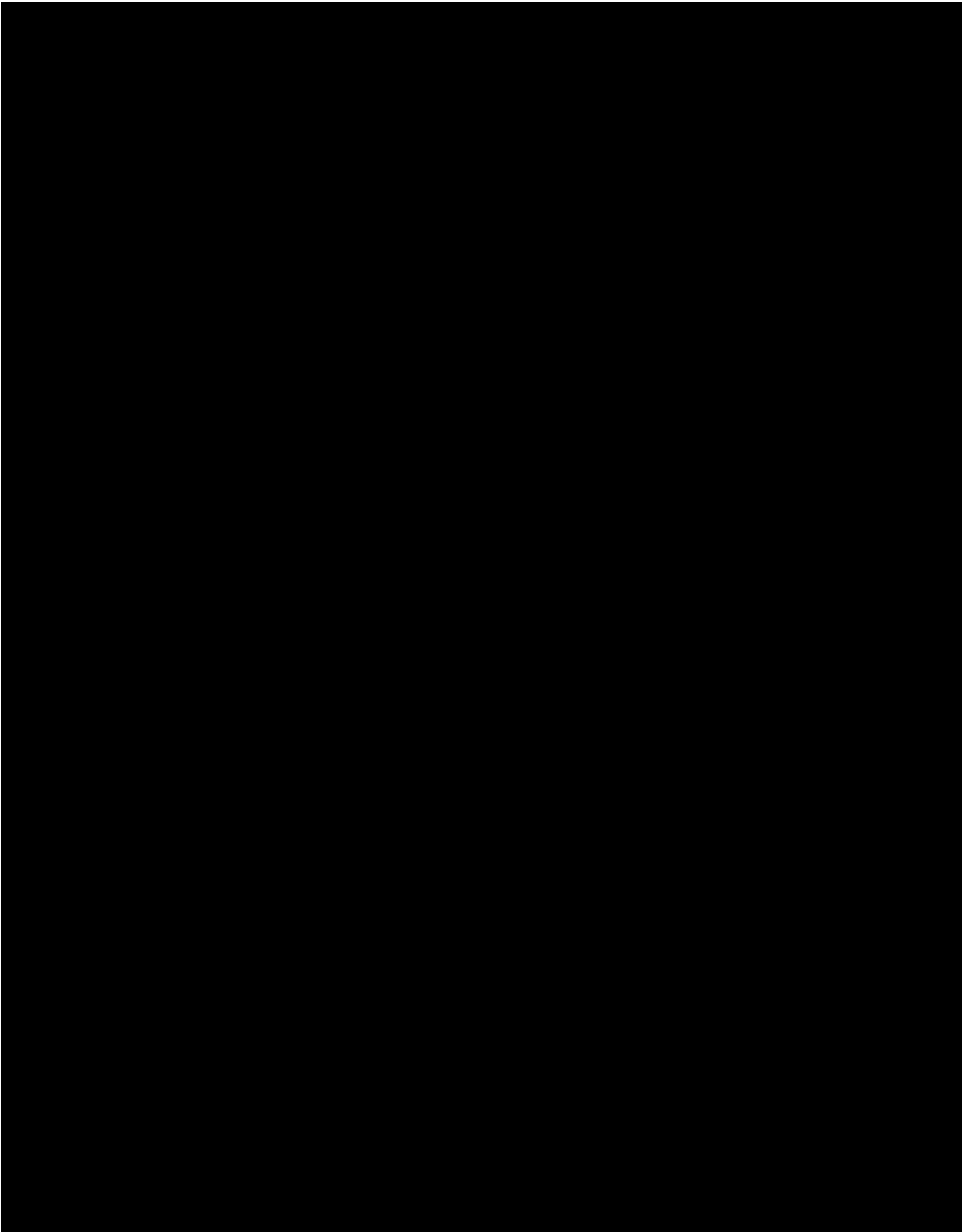


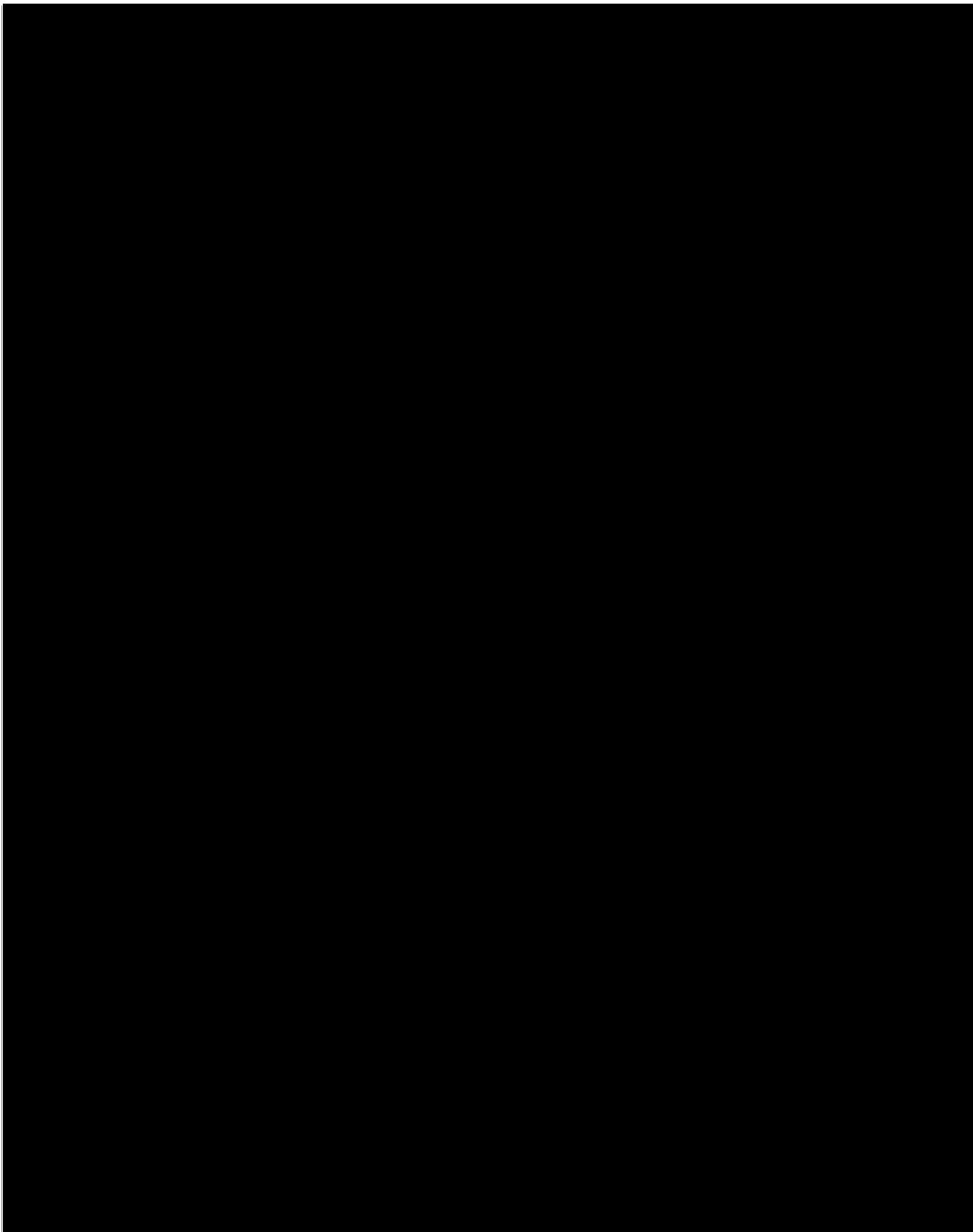


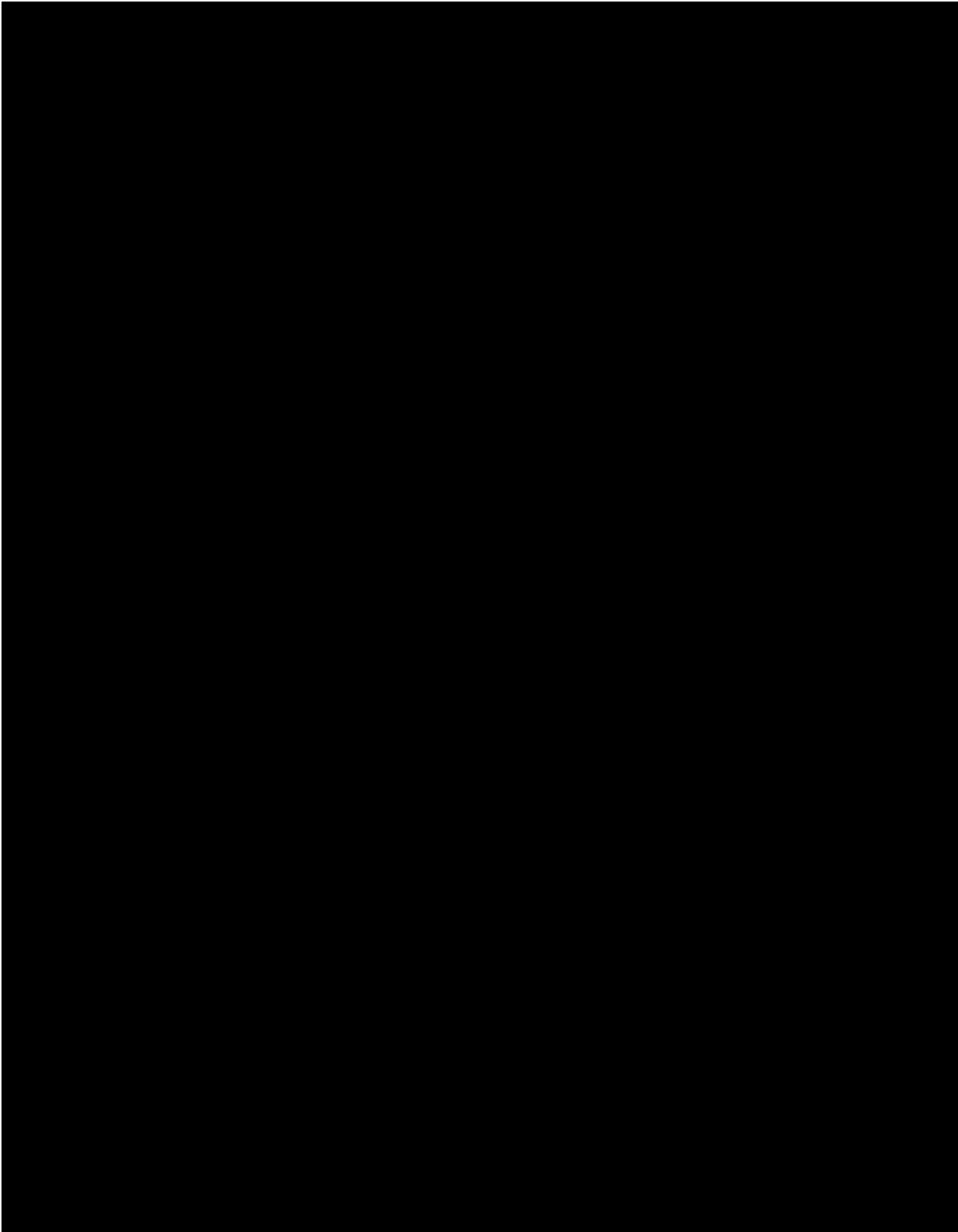












DRAFT

