



16 June 2023

KPMG
Level 38, Tower Three, International Towers Sydney
300 Barangaroo Avenue.
Sydney New South Wales, 2000

ATTENTION: [REDACTED]

Dear [REDACTED]

Re: Letter of Intent in relation to finalisation of an Agreement under the New South Wales Government's Digital NSW ICT Purchasing Contracting Framework (ICTA Agreement) between Macquarie University ABN 90 952 801 237 (the University) and KPMG ABN 51 194 660 183 (collectively, Parties) for the provision of Salesforce Implementation Partner Services (the Services)

We refer to the meeting held on Thursday 25 May 2023 in relation to the above and confirm the following:

1. The University advised KPMG that as a result of the Tender lodged by KPMG in response to the University's Request for Tender for the provision of the Services, KPMG has been nominated as a supplier to provide the Services to the University as part of a preferred supplier panel, subject to successful contract negotiations and execution of an ICTA Agreement.
2. Execution of this Letter of Intent confirms that KPMG agrees to commence preliminary work for the provision of the Services in the form of professional services (the **Preliminary Services**) while negotiations between the University and KPMG on aspects of the terms and conditions of a formal ICTA Agreement for the provision of the Services continue and those terms and conditions are finalised and that the ICTA Agreement is entered into by the University and KPMG.

This Letter of Intent together with the Remote Access Agreement, Statement of Work, Non-Disclosure Agreement (Mutual) and the attached University Policy and Procedures will serve as an interim agreement (**Interim Agreement**) between the University and KPMG. If there is an inconsistency between a provision of the Letter of Intent, Remote Access Agreement, Statement of Work, Non-Disclosure Agreement (Mutual) and University Policies and Procedures, then the provisions of the first mentioned prevail.

The terms of this Interim Agreement are as follows:

1. Subject to paragraphs 3(b) and 3(c), below, the University and KPMG will, in good faith and in a timely manner endeavour to agree on the terms and conditions of the ICTA Agreement (and endeavour to procure that the ICTA Agreement is entered on those agreed terms and conditions by the University and KPMG by **30 September 2023** or

such later date as the University and KPMG may agree in writing from time to time (**Negotiation End Date**). The University and KPMG will each bear their own respective costs and expenses of negotiating and executing the ICTA Agreement.

2. If the ICTA Agreement is not entered into by the Negotiation End Date, this Interim Agreement will terminate and come to an end and no Agreement will exist between the Parties for the continued provision of the Interim Services or for the provision of the Services.
3. The Parties acknowledge and agree that:
 - (a) the scope of the Preliminary Services, the terms and conditions, the manner and timing of the delivery of the Preliminary Services and the amounts payable by the University for the provision of the Preliminary Services (and when those amounts will be payable) will be set out in the attached Statement of Work as amended from time to time (**SOW**);
 - (b) the University may terminate the negotiations referred to in paragraph 1 above at any time;
 - (c) the University reserves the right to commence negotiations with other potential providers of any or all of the Services at any time subject to its confidentiality obligations to KPMG under the Non-Disclosure Agreement executed by the parties and dated 15 March 2023, attached to this agreement and marked Attachment A;
 - (d) if the University terminates the negotiations referred to in paragraph 1 above with KPMG, this Interim Agreement will also terminate at that time;
 - (e) if this Interim Agreement terminates as contemplated by paragraphs 2 or 3(d) above, KPMG will:
 - (i) be entitled to charge the University fees for works completed; and
 - (ii) subject to paragraph 3(f) below, be entitled to charge the University for any allowable expenses incurred by KPMG,

determined as provided in the SOW in respect to the provision by it of any Preliminary Services to the University up to the date of any such termination (to the extent that the University has not previously been charged those fees and expenses in relation to those Preliminary Services in accordance with the SOW) provided those Preliminary Services were delivered to, and accepted by, the University;
 - (f) an expense will not be an allowable expense for the purposes of paragraph 3(e) above unless:
 - (i) it was reasonably necessary for KPMG to incur the particular expense (following discussion and agreement with the University) prior to the ICTA Agreement being signed;
 - (ii) the expense was incurred between the date this Interim Agreement is signed by the University and KPMG and the time that this Interim



Agreement is terminated as contemplated by paragraphs 2 or 3(d) above;
and

(iii) the University gave prior written approval to KPMG incurring that expense;

(g) the University undertakes to provide any University inputs, equipment, resources, materials or dependencies as set out in the relevant SOW.

4. The IT Remote Access Agreement that is attached to this Interim Agreement is incorporated into and forms part of this Interim Agreement. KPMG must, in connection with its provision of the Interim Services, comply with its duties and obligations as the Supplier in that IT Remote Access Agreement.
5. KPMG will at all times during the term of this Interim Agreement comply with its "Information Security at KPMG Australia" policy, and implement, maintain and enforce a program of technical and organisational security measures in compliance with, or equivalent to ISO27001:2013. KPMG will at all times during the term of this Interim Agreement comply with University's policies and procedures when working in the University environment.
6. For the duration of this Interim Agreement, KPMG must ensure that it is covered by the insurance policies whose details were provided in the Tender lodged by KPMG in response to the University's Request for Tender for the provision of the Services.
7. KPMG represents and warrants that the performance of its obligations under this Interim Agreement and the provision by it of the Preliminary Services will not, upon delivery and to the best of its knowledge:
 - (a) breach of any law or mandatory code of conduct;
 - (b) infringe any person's rights (including Intellectual Property and Moral Rights);
 - (c) constitute a misuse of any person's confidential information; or
 - (d) result in KPMG company breaching any obligation that it owes to any person which may materially prevent the University to use the Interim Services.
8. In providing the Interim Services, KPMG must comply with applicable laws, regulations and industry standards as well as any applicable University by-laws, policies, procedures and directions that the University brings to its attention including those relating to security, access to the University's physical and virtual (or online) infrastructure, privacy, health and safety, discrimination and harassment, parking and traffic.
9. This Interim Agreement is intended to operate as an agreement between the University and KPMG, but it will be superseded and come to an end if and when an ICTA Agreement is entered into by the University and KPMG. Interim Services still being performed under a SOW will continue to be performed but will be treated as a SOW under the executed ICTA, including in relation to the obligation to pay fees for those transferred Interim Services. Fees for any Interim Services completed during the term of this Interim Agreement are due and payable on the earlier of the time specified in the relevant SOW or termination of this Interim Agreement.

10. Unless and until an ICTA Agreement is signed by both Parties, no undertaking or representation will arise concerning the Services or the ICTA Agreement, including:
 - (a) that the Parties will reach agreement on the terms and conditions of an ICTA Agreement and enter the ICTA Agreement;
 - (b) as a result of negotiations between the Parties concerning the preparation of the ICTA Agreement; and
 - (c) as a result of any action or inaction by a Party on the assumption or in the expectation that an ICTA Agreement will be executed.
11. For the avoidance of doubt, the parties acknowledge that if an ICTA Agreement is entered into by the University and KPMG, the Interim Services (together with any subsequent services) will form part of the Services that are to be provided under the ICTA Agreement from the date of the ICTA's execution.
12. This Interim Agreement constitutes the entire agreement between the University and KPMG in connection with its subject matter.
13. KPMG may not make any public statement concerning this Interim Agreement or the subject matter of this Interim Agreement, (including the existence of, or any details in relation to, the Services or an ICTA Agreement) without the prior written consent of the University.
14. The law of New South Wales, Australia governs this Interim Agreement, and the University and KPMG submit to the non-exclusive jurisdiction of the courts of New South Wales.
15. This Interim Agreement is intended to be legally binding on the University and KPMG.

Please acknowledge the acceptance and agreement of KPMG to this Letter of Intent by signing and returning the attached copy where indicated.



EXECUTED AS AN AGREEMENT

Signed on behalf of **Macquarie University**
by its authorised officer:


Bruce Dowton (Jun 16, 2023 10:43 GMT+2)

Signature of authorised officer

Bruce Dowton

Name of authorised officer

Vice Chancellor

Position of authorised officer

16/06/23

Date

Signed by **KPMG**



Signature of authorised officer

Julian Edwards

Name of authorised officer

16th June 2023

Date

Attachments:

1. IT Remote Access Agreement
2. Statement of Work
3. Non-Disclosure Agreement (Mutual)
4. University Policies and Procedures

Attachment 1

IT Remote Access Agreement**INFORMATION TECHNOLOGY SYSTEMS
REMOTE ACCESS AGREEMENT****PARTIES****1. MACQUARIE UNIVERSITY**

Full Name	Macquarie University (the University)
------------------	---------------------------------------

ABN	90 952 801 237
------------	----------------

Address for Notices	Balaclava Road Macquarie University NSW 2109
----------------------------	--

Contact Person	Hannah Latham
-----------------------	---------------

Email Address	hannah.latham@mq.edu.au
----------------------	-------------------------

Phone Number	[REDACTED]
---------------------	------------

2. SUPPLIER

Full Name	KPMG (Supplier)
------------------	-----------------

ABN details	51 194 660 183
--------------------	----------------

Address for Notices	Level 38, Tower Three, International Towers Sydney 300 Barangaroo Avenue. Sydney, New South Wales, 2000.
----------------------------	--

Contact Person	[REDACTED]
-----------------------	------------

Email Address	[REDACTED]
----------------------	------------

Phone Number	[REDACTED]
---------------------	------------

BACKGROUND

- A.** The University and the Supplier have entered into the Interim Agreement pursuant to which the Supplier will provide goods or services to the University for or in connection with the IT System or otherwise will have access to the IT System.
- B.** The University has agreed to allow the Supplier to access the IT System on the terms and conditions of this agreement.

OPERATIVE PROVISIONS

1. COMMENCEMENT AND EFFECT

This agreement is supplementary to and forms part of the Interim Agreement and relates to the provision of Preliminary Services and includes the Statement of Work.

2. GRANT OF ACCESS RIGHTS

2.1 Grant of Access Rights

The University grants the Supplier a non-exclusive, non-transferable right to access the IT System remotely for the Permitted Purpose on the terms and conditions of this agreement.

2.2 Acceptance

The Supplier accepts access to the IT System on the terms and conditions of this agreement.

3. RESTRICTIONS ON SUPPLIER'S ACCESS TO THE IT SYSTEM

3.1 Directions and Policies

(a) The University may, during the Term of this agreement:

- (i) issue reasonable directions in relation to or limitations on the Supplier's right to access the IT System; and
 - (ii) issue Policies,
- as it considers necessary or appropriate.

(b) The Supplier must:

- (i) comply with all reasonable directions, limitations and applicable Policies notified to it by the University when accessing the IT System; and
- (ii) notify the University promptly if it becomes aware of a breach of any of the Policies by it or its Personnel.

3.2 Restrictions on Supplier's Access Rights

Without limitation to the Supplier's obligations under clause 3.1(b), when accessing the IT System, the Supplier must only undertake those acts which would be considered by the University (acting reasonably) as constituting part of an acceptable or normal access process for the purposes for which the Supplier is accessing the IT System.

3.3 Suspension or Revocation of Rights

(a) The University may suspend or revoke the Supplier's or any of its Personnel's rights to access the IT System as it considers necessary or appropriate in its absolute discretion.

- (b) The Supplier will not be liable to the University for any failure by it to provide Support under the Interim Agreement to the extent that failure arises due to the suspension or revocation under paragraph (a) of this clause of the rights of the Supplier or any of its Personnel to access the IT System in circumstances where that suspension or revocation was instituted for reasons other than a breach by the Supplier or any of its Personnel of their duties and obligations under this agreement and/or the Interim Agreement (and the University will not be entitled to terminate the Interim Agreement due to any such failure in these circumstances).
- (c) The Supplier acknowledges that it may be liable to the University for any failure by it to provide the Preliminary Services under the Interim Agreement as a result of the suspension or revocation under paragraph (a) of this clause in circumstances where that suspension or revocation was instituted by the University in whole in response to a material breach by the Supplier or any of its Personnel of their duties and obligations under this agreement and/or the Interim Agreement (and the University may potentially be entitled to terminate the Interim Agreement due to any such failure in these circumstances).

3.4 Confidential Information

- (a) Each party acknowledges that the Confidential Information of the other party is valuable to the other party. Each party undertakes to keep the Confidential Information of the other party secret and to protect and preserve the confidential nature and secrecy of the Confidential Information of the other party.
- (b) A Recipient may only use the Confidential Information of the Discloser for the purposes of performing the Recipient's obligations or exercising the Recipient's rights under this Agreement.
- (c) Subject to paragraph (d) of this clause, a Recipient may not disclose Confidential Information of the Discloser or the existence or contents of this Agreement to any person except:
 - (i) Personnel of the Recipient who require it for the purposes of the Recipient performing its obligations or exercising its rights under this Agreement and then only on a need-to-know basis;
 - (ii) with the prior written consent of the Discloser;
 - (iii) if the Recipient is required to do so by law or a stock exchange or to the extent necessary to comply with applicable professional and ethical standards or codes, or where required by a regulator to do so; or
 - (iv) if the Recipient is required to do so in connection with legal proceedings relating to this agreement or the Interim Agreement.
- (d) A Recipient disclosing information under sub-paragraphs (c)(i) or (c)(ii) of this clause must ensure that persons receiving Confidential Information from it are aware it is the other party's Confidential Information and do not disclose the information except in the circumstances permitted in paragraph (c) of this clause.
- (e) Subject to paragraph (f) of this clause, on the Discloser's request, the Recipient must immediately deliver to the Discloser all documents or other materials containing or referring to the Discloser's Confidential Information (or if in electronic form, erase or destroy and deliver evidence of erasure or destruction) which are:
 - (i) in the Recipient's possession, power or control; or

- (ii) in the possession, power or control of persons who have received Confidential Information from the Recipient under sub-paragraphs (c)(i) or (c)(ii) of this clause.
- (f) The obligation in paragraph (e) of this clause does not apply to Confidential Information of the Discloser that the Recipient requires to perform its obligations under this agreement and the Interim Agreement, for quality assurance and risk management purposes or is otherwise entitled to retain.

3.5 Personal Information

Each party must:

- (a) comply with applicable Privacy Laws and mandatory codes;
- (b) not collect, use, process, handle, transfer or disclose the Personal Information other than for the purpose of performing its obligations under this agreement and the Interim Agreement;
- (c) take such steps as are reasonable in the circumstances to ensure that the Personal Information is protected against misuse, interference and loss, and from unauthorised access, modification or disclosure;
- (d) not access, transfer, take, send, store or allow the storage of outside Australia of any Personal Information it receives (or in respect to which it gains access) other than as a consequence of or in the performance of its rights and obligations under this agreement or the Interim Agreement and not disclose or allow the disclosure of that Personal Information to any person outside Australia other than as required for the purposes of providing the support services under this agreement or the Interim Agreement or as otherwise agreed in writing by parties;
- (e) promptly notify the other party in writing (and in any event within 48 hours of becoming aware), and give a summary of the details, if it becomes aware of any grounds to believe or suspect that there has been any misuse, interference and loss from any unauthorised access, modification to or disclosure or loss of Personal Information in its possession, custody or control, (a "**Notifiable Incident**"). Each notification must (to the extent then known) include the nature and details of the Notifiable Incident, the kinds of Personal Information affected (or suspect to be affected) and recommendations for any actions to be taken by the Supplier, the University and/or individuals who are or may be affected by the Notifiable Incident;
- (f) promptly (and in any event within no more than thirty (30) days of being requested by the other party:
 - (i) investigate and complete an expeditious assessment of the Notifiable Incident, including the possible impacts of the Notifiable Incident and likelihood of harm to any individuals to whom the information relates;
 - (ii) report to the other party a summary of the results of such investigation and assessment and any updates to the information and recommendations referred to in paragraph (e) of this clause;
 - (iii) provide all reasonable assistance requested by the other party in relation to its own investigation, assessment and management of the Notifiable Incident;
 - (iv) be open to the other party's reasonable directions in connection with how the Notifiable Incident is being managed, assessed, or reported, including to relevant regulatory authorities and/or individuals who are or may be affected by the

Notifiable Incident (as applicable); and

- (v) take all appropriate or necessary remedial action reasonably within that party's control to mitigate any potential loss or interference with Personal Information, preventing any further harm and protecting the Personal Information from further misuse, loss, access or disclosure.

Without limiting the Supplier's obligations under the rest of this clause 3.5, to the extent permitted by law, the parties agree that the party with the most direct relationship with the individuals who are or may be affected by the Notifiable Incident should undertake the notification to those individuals and/or the relevant regulatory authority (including determining the form and content of any such notice(s)).

3.6 Supplier's dealing with the University Data

The Supplier must:

- (a) not use, disclose or deal with the University Data other than for the purpose of performing this agreement and the Interim Agreement and exercising its rights;
- (b) take such steps as are reasonable in the circumstances to ensure that the University Data is protected against misuse, interference and loss, and from unauthorised access, modification or disclosure;
- (c) promptly notify the University in writing, and provide a written summary, of any breach of this clause 3.6 that materially affects the University Data;
- (d) not sell, loan or otherwise provide the University Data or Improvements to any third party, without the University's express prior written consent, and
- (e) not use University's name or logo without the prior written consent of the University.

3.7 Supplier Must Return or Destroy Documents

On written demand from the University, the Supplier must, at the option of the University, and subject to the Supplier's legal and regulatory data retention obligations:

- (a) promptly return or destroy all documents in its possession or control which contain any Confidential Information or Personal Information (provided however the Supplier may retain its work papers, that may contain the University's Confidential Information, for quality assurance and risk management purposes); and
- (b) promptly return, destroy or de-identify all Personal Information in its possession or control.

3.8 Confidentiality Obligations Continue

Except to the extent that documents referred to in clause 3.7 are needed by the Supplier to perform its obligations under the Interim Agreement, the return or destruction of documents under clause 3.7 does not release the Supplier from its other obligations under this agreement or the Interim Agreement.

4. SYSTEM ACCESS

4.1 Method of Access to the IT System

The Supplier will be granted access to relevant parts of the University's IT System at such times

and in such manner as the University and the Supplier may agree in writing from time to time.

4.2 Restrictions on Access to the IT System

- (a) The Supplier must not allow any person other than the Designated Personnel, the Essential Personnel (and such other Personnel of the Supplier as the University may approve in writing from time to time) to access the IT System.
- (b) The Supplier must ensure that the IT System is only used and accessed by it and its Personnel referred to in paragraph (a) of this clause solely for the Permitted Purpose.
- (c) The Supplier warrants that it has all necessary consents from each of its Personnel to disclose that person's name and other identifying information to the University.

4.3 Ceasing Employment

The Supplier must inform the University when any Designated Personnel, Essential Personnel or other Personnel who have been given access to IT System cease their employment or independent contractor arrangements with the Supplier.

4.4 Record Keeping and Reporting

- (a) The Supplier agrees to keep records of its Personnel who access the IT System. The records must include, as a minimum, the following information in respect of any such Personnel:
 - (i) the full name of the Personnel;
 - (ii) the Personnel's role within the Supplier's organisation;
 - (iii) the Personnel's role in relation to the supply of goods or services to the University;
 - (iv) the purpose for which the Personnel accessed the IT System.
- (b) At no cost to the University, the Supplier will:
 - (i) if requested by the University, provide a copy of the records referred to in paragraph (a) of this clause;
 - (ii) provide any relevant information requested by the University within a reasonable time of the University's request; and
 - (iii) discuss with representatives of the University within seven days of the University's request any issues arising from the records.

5. SUPPLIER'S PERSONNEL

5.1 Compliance by Personnel and Advisers

Without limitation to any other clause of this agreement, the Supplier must procure that all its Personnel who are given access to the IT System, comply with the terms of this agreement.

5.2 Supplier Responsible for Personnel

The Supplier is responsible and accepts liability for the acts and omissions of its Personnel that cause damage to the University.


6. LIABILITY

6.1 Liability

(a) 

(b) The liability of a party under clause 6.1(a) does not apply to:

(i) in the case of the Supplier:

- (A) breach of a duty of confidentiality owed by the Supplier to the University under this Interim Agreement; or
 - (B) breach of clause 3.6 of this Information Technology Systems Remote Access Agreement,
- 

(ii) the following for which the liability of a party is uncapped:

- (A) personal injury, illness or death caused or contributed to by any act or omission of that party;
- (B) damage to any real or tangible property caused or contributed to by any act of that party;
- (C) breach of clause 8.7(a)(ii) of this Information Technology Systems Remote Access Agreement;
- (D) any liability that cannot by Law be limited or excluded; or
- (E) in respect of the Supplier, any fraud or Wilful Misconduct of the Supplier or its Personnel.

(c) Each party's liability will be reduced proportionately to the extent caused or contributed by the other party.

(d) A party must take all reasonable steps to mitigate its loss or damage arising under or in connection with this Interim Agreement.

6.2 Liability principles

Each party agrees and acknowledges that:

- (a) neither party is liable to the other party under or in connection with this Agreement for any Excluded Loss; and
- (b) neither party is entitled to make more than one Claim for the same loss or damage arising from the same event.

7. INDEMNITY

7.1 Supplier indemnities

- (a) The Supplier must at all times indemnify and defend the University and its Personnel against all Loss incurred by University or its Personnel where such Loss is caused by the Supplier as a result of:
 - (i) personal injury, illness or death cause or contributed to by any act or omission of the Supplier and its Personnel;
 - (ii) damage to any real or tangible property caused or contributed to by any act of the Supplier or its Personnel;
 - (iii) fraud or Wilful Misconduct under this Interim Agreement.
- (b) The indemnities contained in this clause 7.1:
 - (i) are a continuing obligation of the Supplier;
 - (ii) are separate and independent of any other responsibility or obligation of the Supplier.

8. Intellectual property

8.1 Ownership of Existing Materials

The parties agree that nothing in this Agreement will affect the ownership of the Intellectual Property Rights in any Existing Materials. The parties will create a schedule of Existing Materials belonging to each party which will form an attachment to the SOW.

8.2 Licence to use Existing Materials

- (a) The Supplier grants to the University an irrevocable, non-exclusive, worldwide, transferable, royalty-free licence to use, copy, adapt, translate, reproduce, modify, communicate and distribute any Intellectual Property Rights in the Supplier's Existing Materials for any purpose in connection with the:
 - (i) University performing its obligations and exercising its rights under this Agreement; or
 - (ii) full use of any Services and/or Deliverables in which the Supplier's Existing Material is incorporated, including installing, operating, upgrading, modifying, supporting, enhancing and maintaining the Deliverables or integrating them with any other software, systems, equipment or infrastructure owned, operated or maintained by the University.
- (b) The rights and licences granted by the Supplier to the University in clause 8.2(a):
 - (i) do not permit the University to sell, monetise or commercialise the Supplier's Existing Materials; and
 - (ii) are sub-licensable by the University (on the same terms, for the same period and for the same purposes as set out in clause 8.2(a)), without additional charge to any:
 - a. controlled entity of Macquarie University (as defined in s16A of the Macquarie University Act 1989 (NSW), contractor, subcontractor or outsourced service provider (subject to such persons being under reasonable obligations of confidentiality owed to the University) acting on behalf of, or providing products and/or services for the benefit of, the University.

- (c) The University grants to the Supplier, a non-exclusive, non-transferable, revocable, worldwide, royalty-free licence to use the Intellectual Property Rights in the University's Existing Materials, to the extent required for the Supplier to perform, and solely for the purposes of the Supplier performing, its obligations under this Agreement.

8.3 Ownership of New Materials

- (a) Where the Supplier creates New Materials in carrying out the services, then, subject to clause 8.3(b), the ownership of all Intellectual Property Rights in those New Materials vests in, or is transferred or assigned to, the Supplier immediately on creation.
- (b) Where the University is of the reasonable opinion that the New Materials are University New Materials, then the parties will promptly escalate that matter to the IP Governance Forum to determine ownership of those New Materials in accordance with the IP Governance Plan.
- (c) Where a matter is referred to the IP Governance Forum under clause 8.3(b), and the IP Governance Forum determines that the New Materials are University New Materials, then:
 - (i) the ownership of all Intellectual Property Rights in those University New Materials is taken to have vested in, or transferred or assigned to, the University on creation;
 - (ii) the University New Materials become and are taken to be University Confidential Information; and
 - (iii) the University grants to the Supplier a non-exclusive, worldwide, non-transferable, royalty-free licence to use, copy, adapt, translate, reproduce, modify, communicate and distribute the Intellectual Property Rights in the University New Materials, for the purpose of performing the services and delivering the Deliverables under this Interim Agreement and the ICTA.

8.4 University licence to use Supplier owned New Materials

- (d) Where the Supplier owns the Intellectual Property Rights in any New Materials, the Supplier grants to the University an irrevocable, non-exclusive, worldwide, transferable, royalty-free licence to use, copy, adapt, translate, reproduce, modify, communicate and distribute the Intellectual Property Rights in such New Materials, for any purpose in connection with the:
 - (iv) University performing its obligations and exercising its rights under this Agreement; or
 - (v) full use of any Services and/or Deliverables in which New Material is incorporated, including installing, operating, upgrading, modifying, supporting, enhancing and maintaining the Deliverables or integrating them with any other software, systems, equipment or infrastructure owned, operated or maintained by the University.
- (e) The rights and licences granted by the Supplier to the University under clause 8.4(a) are sub-licensable by the University (on the same terms and for the same purposes as set out in those clauses) to any person, without additional charge, including to any:
 - (i) contractor, subcontractor or outsourced service provider (subject to such persons being under reasonable obligations of confidentiality owed to the University acting on behalf of, or providing products and/or services for the benefit of, the University

8.5 Licence term

The licences granted under clauses 8.2 and 8.4 will be perpetual in relation to the purposes specified in those clauses and those clauses, along with clauses 8.1 and 8.3, this clause 8.5 and clause 8.8, survive termination of this Interim Agreement.


8.6 Consents and Moral Rights

Prior to provision to the University or use in connection with this Agreement, the Supplier must ensure that it obtains all necessary consents from all authors of all Materials and Deliverables provided or licenced to the University under this Principal Agreement to any use, modification or adaptation of such Materials and Deliverables to enable the University to fully exercise its Intellectual Property Rights under this Principal Agreement.

8.7 Warranties and acknowledgements

- (a) The Supplier represents, warrants and undertakes that:
- (i) it has all the Intellectual Property Rights and has procured the necessary Moral Rights consents required to:
 - A. carry out the services; and
 - B. enable the University or its other permitted licensee to use the requisite Services and/or Deliverables in the manner envisaged by this Interim Agreement; and
 - (ii) its supply of the requisite services and/or Deliverables to the University, and the Customer's other permitted licensees' use of them in the manner envisaged by this Principal Agreement will not infringe the Intellectual Property Rights or Moral Rights of any third party.
- (b) The Supplier acknowledges and agrees that the Intellectual Property Rights and licences (as applicable) granted under this Agreement (including this clause 8) do not limit or reduce the Supplier's or its Personnel's obligations under this Principal Agreement with respect to the University's Confidential Information, Personal Information and University Data.

8.8 IP Governance Forum

- (a) The parties will:
- (i) meet in good faith to agree a governance plan for the review of New Materials in accordance with clause 8.3(b) (**IP Governance Plan**); and
 - (ii) 
- (b) The IP Governance Plan will address the following:
- (i) establishment of an IP Governance Forum;
 - (ii) role and responsibilities of the IP Governance Forum;
 - (iii) each party's nominated representative who are required to attend the IP Governance Forum;
 - (iv) the representative who is required to chair the IP Governance Forum and what role that individual has;
 - (v) how meetings will be conducted, including location and video conferencing, minute taking, record keeping and reporting;

- (vi) the criteria for assessing whether the New Materials are University New Materials;
 - (vii) timeframe for decisions and when those decisions of the IP Governance Forum are deemed binding on the parties;
 - (viii) in what circumstances a matter is considered as not agreed by the parties and should be referred to dispute resolution; and
 - (ix) any other matters the parties agree in writing.
- (c) Where the parties are unable to reach agreement on a matter referred or escalated under clause 8.3(b) in the timeframe provided in the IP Governance Plan, then the matter will be considered a dispute and referred for dispute resolution in accordance with clause 35 of the ICTA.
- (d) The IP Governance Forum is in addition to any other agreed governance framework for the provision of the services under this Interim Agreement or the ICTA.

9. DEFINITIONS AND INTERPRETATION

9.1 Definitions

In this agreement unless the context otherwise requires:

Claim means any actions, suits, causes of action, proceedings, claims or demands whatsoever.

Commencement Date means the date specified on the first page of this agreement as the date on which the parties signed this agreement and if the parties signed the agreement on different dates, the latter of the two dates.

Confidential Information in relation to the University means all information specified in any applicable Policy as being the confidential information or proprietary data of the University or any information which is provided by or on behalf of the University to the Supplier or to which the Supplier has access of any nature and in any form for or in connection with the Permitted Purpose including any information and material which is copied or derived from such, or in relation to the Supplier, all information exchanged under this agreement which shall be deemed confidential if disclosed in any form or manner, marked or reasonably considered confidential, including but not limited to information relating to research, activities, products, software, services, data, techniques, strategies, personnel information, processes, etc.. Confidential Information shall also include the existence of as well as the terms and conditions of this agreement and any order placed hereunder, but does not include information which:

- (a) is or becomes readily available in the public domain, other than as a result of a breach of this agreement or any other confidentiality obligations by the Recipient or any of its Personnel;
- (b) is known to the Recipient before it received it and is not subject to an existing obligation of confidence between the parties; or
- (c) is independently developed or acquired by the Recipient as established by written evidence.

Deliverable means all things or items (including Documents) to be supplied by the Supplier under this Agreement as set out in the SOW.

Designated Personnel means a named member of the Personnel of the Supplier who the University and the Supplier agree will be used by the Supplier to provide goods or services to the University under the Interim Agreement.

Discloser means the party disclosing Confidential Information.

Essential Personnel means a Personnel of the Supplier (other than a Designated Personnel) who requires access to the IT System to allow the Supplier to undertake the Permitted Purpose.

Excluded Loss means any special, indirect or consequential Loss arising under or in connection with this Agreement, including any:

- (a) loss of profits;
- (b) loss of sale of business;
- (c) loss of business opportunity;
- (d) loss of anticipated savings;
- (e) loss of or damage to goodwill, and
- (f) loss of reputation.

Existing Materials means any Materials in which Intellectual Property Rights subsist (which, in the case of the Supplier, are incorporated into a Deliverable or Service or to which the University otherwise requires a licence in order to enjoy the benefit of this Agreement or any obligations performed for the University under it):

- (a) belonging to a party that are pre-existing as at the Commencement Date; or
- (b) that are brought into existence, by or on behalf of a party, other than in connection with the performance of that party's obligations under this Agreement,

and includes any enhancements, modifications and developments to such Materials, to the extent not comprising New Materials.

Improvements means any transformation, modification, translation version, enhancement or advancement, variation or configuration of or to the University Data which is developed or updated during the course of this Agreement.

Intellectual Property Rights means all intellectual property rights, including:

- (a) copyright, patent, design, semi-conductor or circuit layout rights, registered design, trade marks or trade names and other protected rights, or related rights, existing worldwide; and
- (b) any licence, consent, application or right to use or grant the use of, or apply for the registration of, any of the rights referred to in paragraph (a),

but does not include the right to keep Confidential Information confidential, Moral Rights, business names, company names or domain names.

IP Governance Forum means the governance forum established under the Governance Plan.

IP Governance Plan has the meaning given in clause 8.8(a)(i).

IT System means the University's information technology systems including the Confidential Information and data stored in the University's information technology systems and related information, data or systems.

Loss means liabilities, expenses, charges, claims, losses, damages and costs (including reasonable legal costs), proceeding, action, whether based on common law, equity or statute.

Materials means all property, materials, documents, information and items in whatever form, and includes equipment, hardware, computer software (including development tools and object libraries), concepts, approaches, tools, methodologies, processes, know-how, data, documentation, manuals and anything else which is the subject matter of Intellectual Property Rights.

Moral rights means a person's moral rights as defined in the *Copyright Act 1968* (Cth) and any other similar rights existing under any other laws.

New Materials means Materials in which Intellectual Property Rights subsist that are created or which arise in the course of performing this Principal Agreement, excluding University Data.

Permitted Purpose means providing professional services to or otherwise complying with or exercising the Supplier's rights under the Interim Agreement.

Personal Information means personal information or health information as defined in the Privacy Laws in respect to which a party to this agreement gains access as a consequence of or in the performance of its rights and obligations under this agreement or the Interim Agreement.

Personnel means any director, officer, employee, agent or subcontractor of the Supplier.

Policy means any policy or statement issued by the University in connection with its operations including policies relating to Personal Information, Confidential Information, IT System security, network security, data and information security and change control procedures that are applicable to the subject matter of this agreement.

Privacy Laws means:

- (a) the *Privacy Act 1988* (Cth);
- (b) the *Privacy and Personal Information Protection Act 1998* (NSW); and
- (c) the *Health Records and Information Privacy Act 2002* (NSW).
- (d) GDPR.

Recipient means the party receiving Confidential Information.

University Data means all data and information in whatever form that is, of the University including Personal Information disclosed and includes Improvements to the Data:

- (a) disclosed, collected, accessed, used or processed by the Supplier in the course of performing this agreement and the Interim Agreement as such is provided by the University, granted access to or made available, and owned by the University; or
- (b) provided by or on behalf of the University to the Supplier,
but does not include the Supplier's pre-existing intellectual property.

University New Materials means those New Materials that are assessed and agreed by the IP Governance Forum as incorporating University Existing Material that is commercial in confidence to the University, and Materials that provide the University with its unique competitive advantage in the higher education sector.

Wilful Misconduct means a deliberate act or omission of the Supplier, which the Supplier knew or ought reasonably to have known, had it given due consideration to the consequences of such act or omission, would have a materially adverse effect on the University and the Supplier nevertheless deliberately performed that act or omitted to act.

9.2 Interpretation

The following rules apply in interpreting this agreement, except where the context makes it clear that a rule is not intended to apply.

- (a) A reference to:
 - (i) legislation (including subordinate legislation) is to that legislation as amended, re-enacted or replaced, and includes any subordinate legislation issued under it;
 - (ii) a party to this agreement or to any other document or agreement includes a permitted substitute or a permitted assign of that party;
 - (iii) a person includes any type of entity or body of persons, whether or not it is incorporated or has a separate legal identity, and any executor, administrator or successor in law of the person; and
 - (iv) anything (including a right, obligation or concept) includes each part of it.
- (b) A singular word includes the plural, and vice versa.
- (c) If a word is defined, another part of speech has a corresponding meaning.
- (d) If an example is given of anything (including a right, obligation or concept), such as by saying it includes something else, the example does not limit the scope of that thing.
- (e) Headings are for convenience only, and do not affect interpretation.

9.3 Entire Agreement

This agreement is the entire agreement of the parties on the subject matter. The only enforceable obligations and liabilities of the parties in relation to the subject matter are those that arise out of the provisions contained in this agreement. All representations, communications and prior agreements in relation to the subject matter are merged in and superseded by this agreement.

9.4 Prohibition of assignment

- (a) The Supplier may only dispose of, declare a trust over or otherwise create an interest in its rights under this agreement with the prior written consent of the University, such consent not to be unreasonably withheld.
- (b) The University may only dispose of, declare a trust over or otherwise create an interest in its rights under this agreement with the prior written consent of the Supplier, such consent not to be unreasonably withheld.

9.5 Waiver

- (a) Waiver of a breach of this agreement or of any rights created by or arising upon default under this agreement can only be effected in writing and must be signed by the party granting the waiver.
- (b) A breach of this agreement is not waived by a failure to exercise, a delay in exercising, or a partial exercise of, any remedy available under this agreement or in law or equity.

9.6 Operation of this Agreement

Any provision of this agreement, which is unenforceable or partly unenforceable is, where possible, to be severed to the extent necessary to make this document enforceable.

9.7 Amendments

If the parties want to vary this agreement they may do so, but only by a document signed by an authorised representative of each party.

9.8 Notices

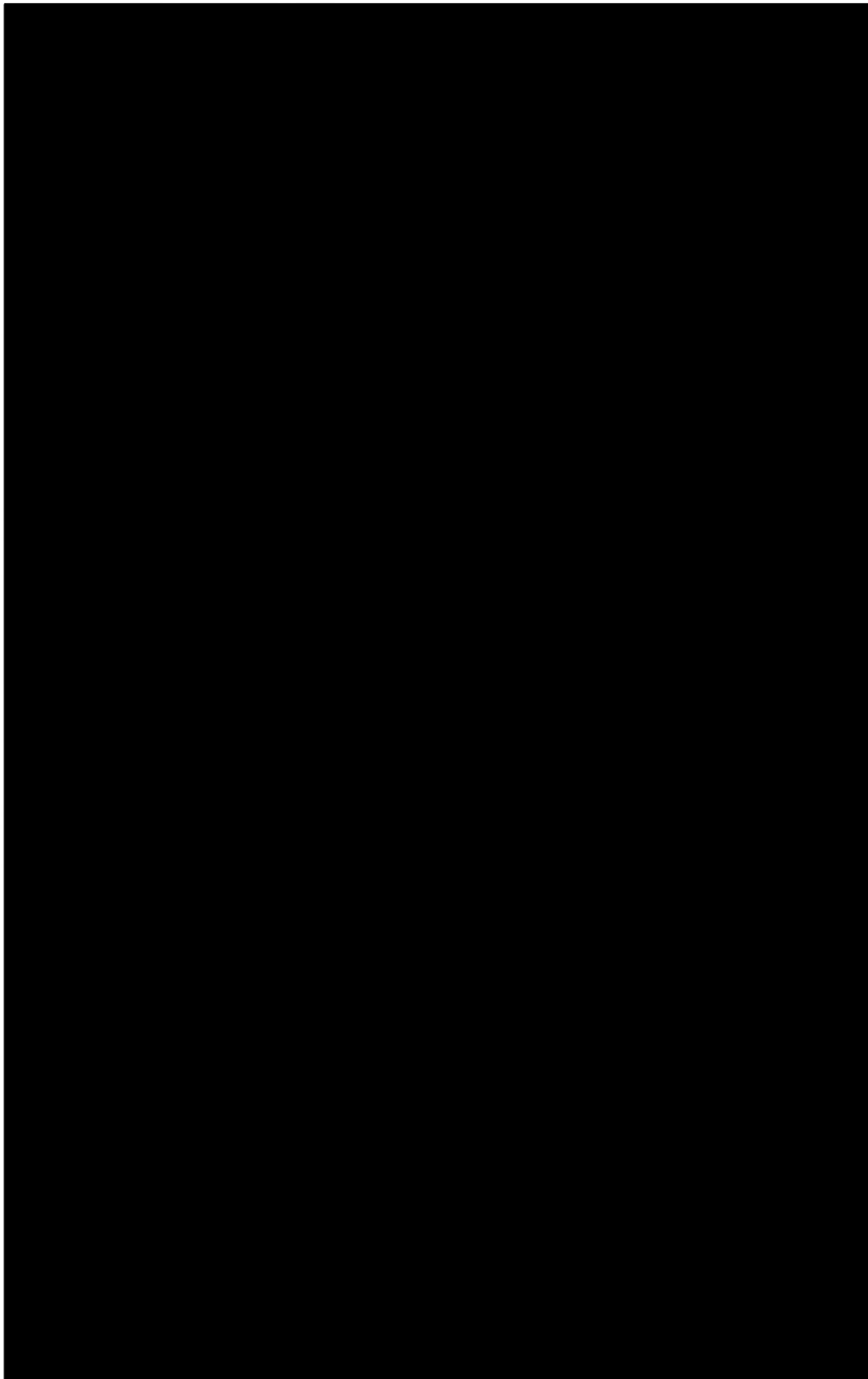
- (a) A notice, consent or other communication under this agreement is only effective if it is:
- (i) in writing and signed by the party's Contact Person specified on the first page of this agreement (or as updated in accordance with this clause 7.8); and
 - (ii) is marked to the attention of the party's Contact Person and is delivered to the recipient by hand, pre-paid post or by email at the address shown on the first page of this agreement.

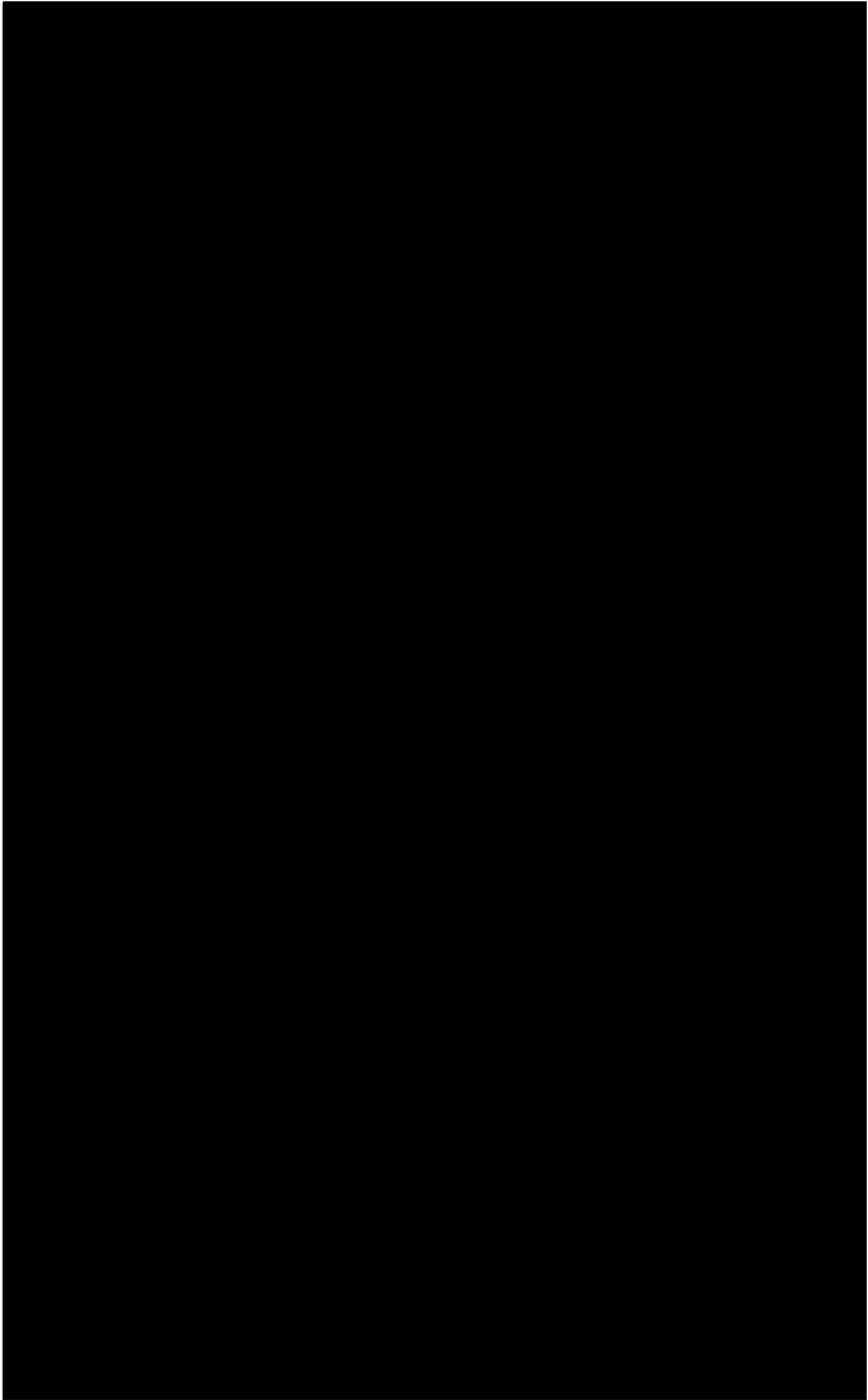
A notice will be effective once received, and will be deemed to be received, if posted in Australia, on the seventh business day in the state or territory where it is addressed to or, if emailed, at the time at which the sender receives a message from the recipient's computer system indicating that the email has been delivered to the recipient's computer system (irrespective of whether the message has been opened by the recipient).

9.9 Governing Law

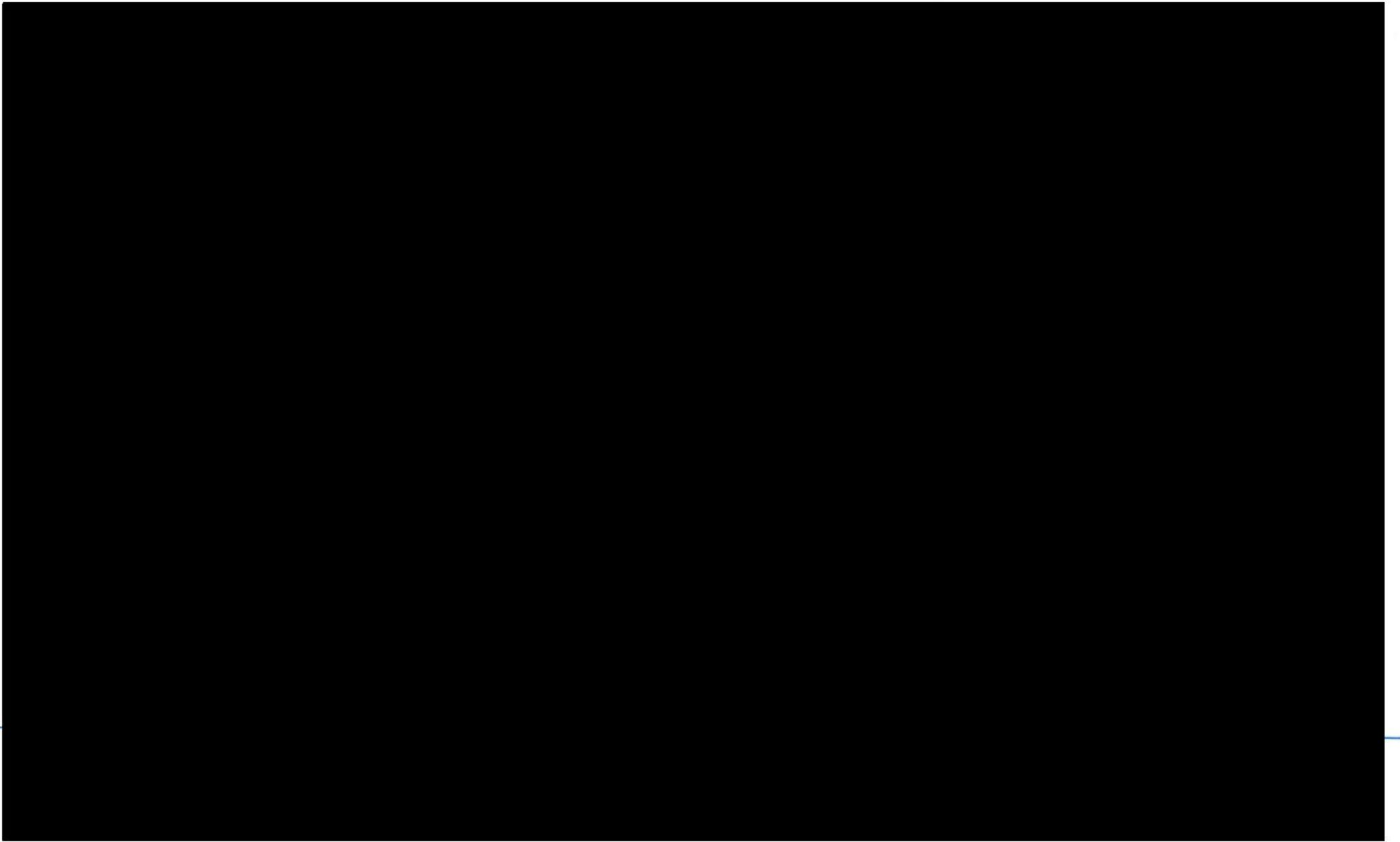
This agreement is governed by the law applicable in New South Wales, Australia and each party irrevocably and unconditionally submits to the non-exclusive jurisdiction of the Courts of that state.

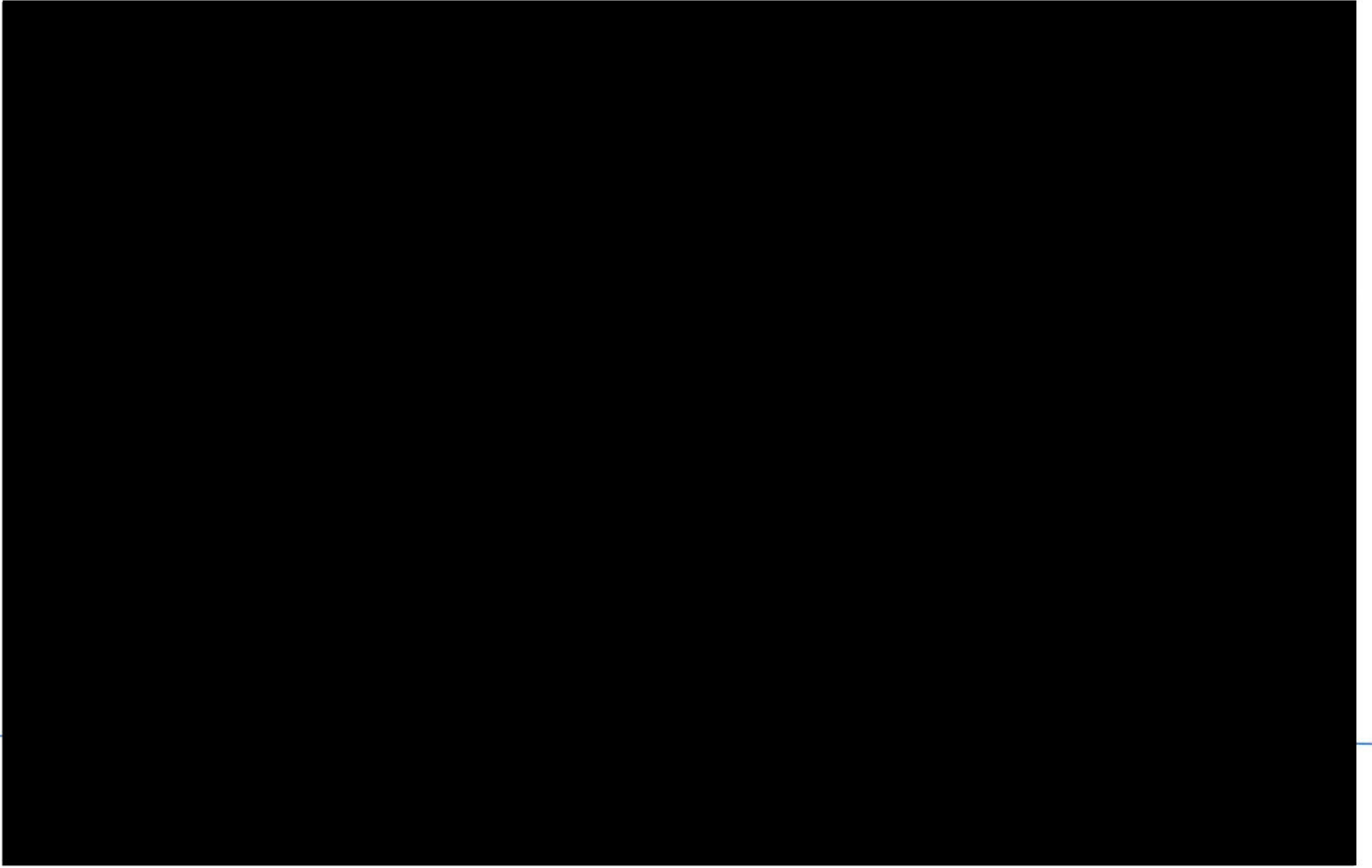
Attachment 2
Statement of Work

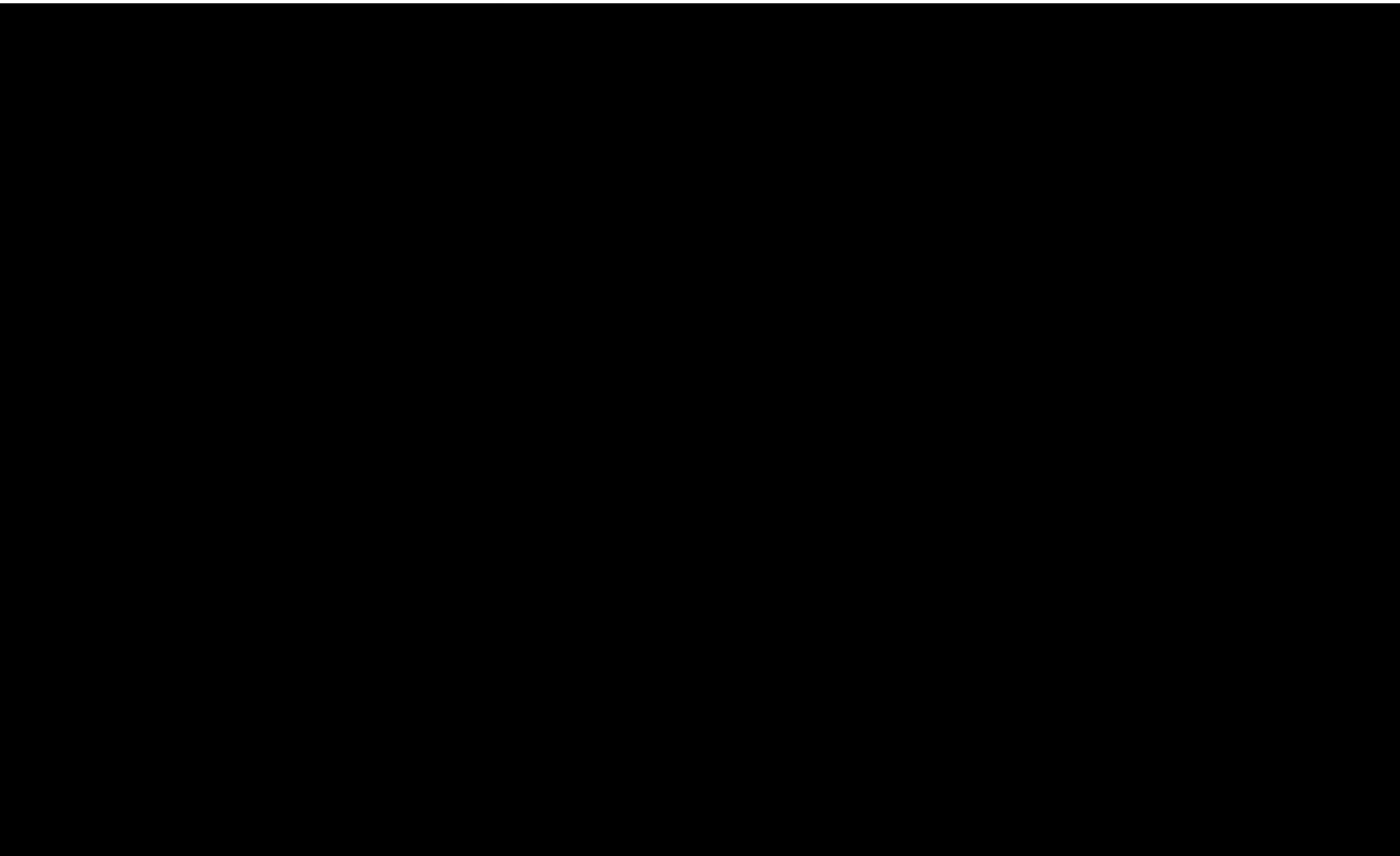


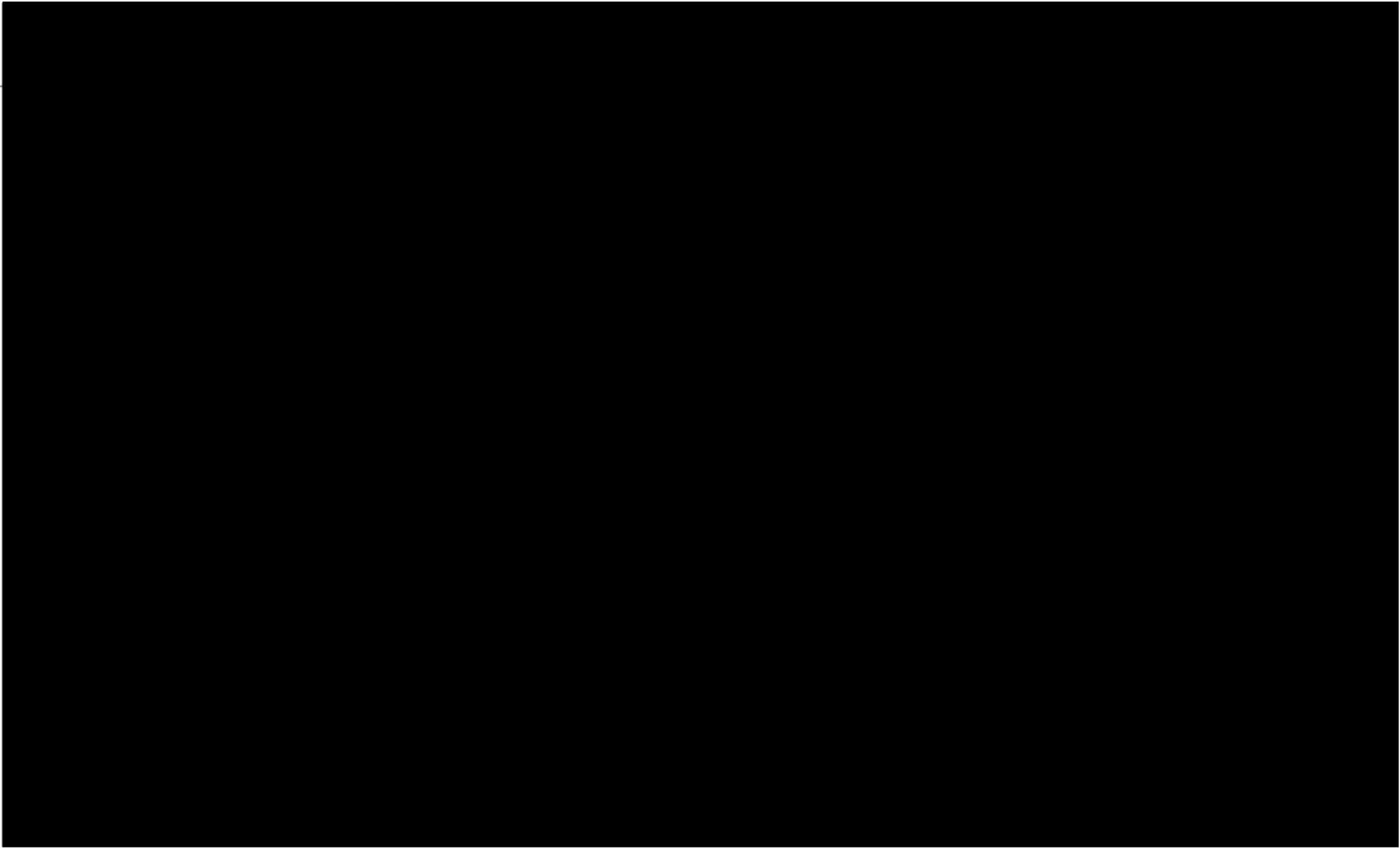








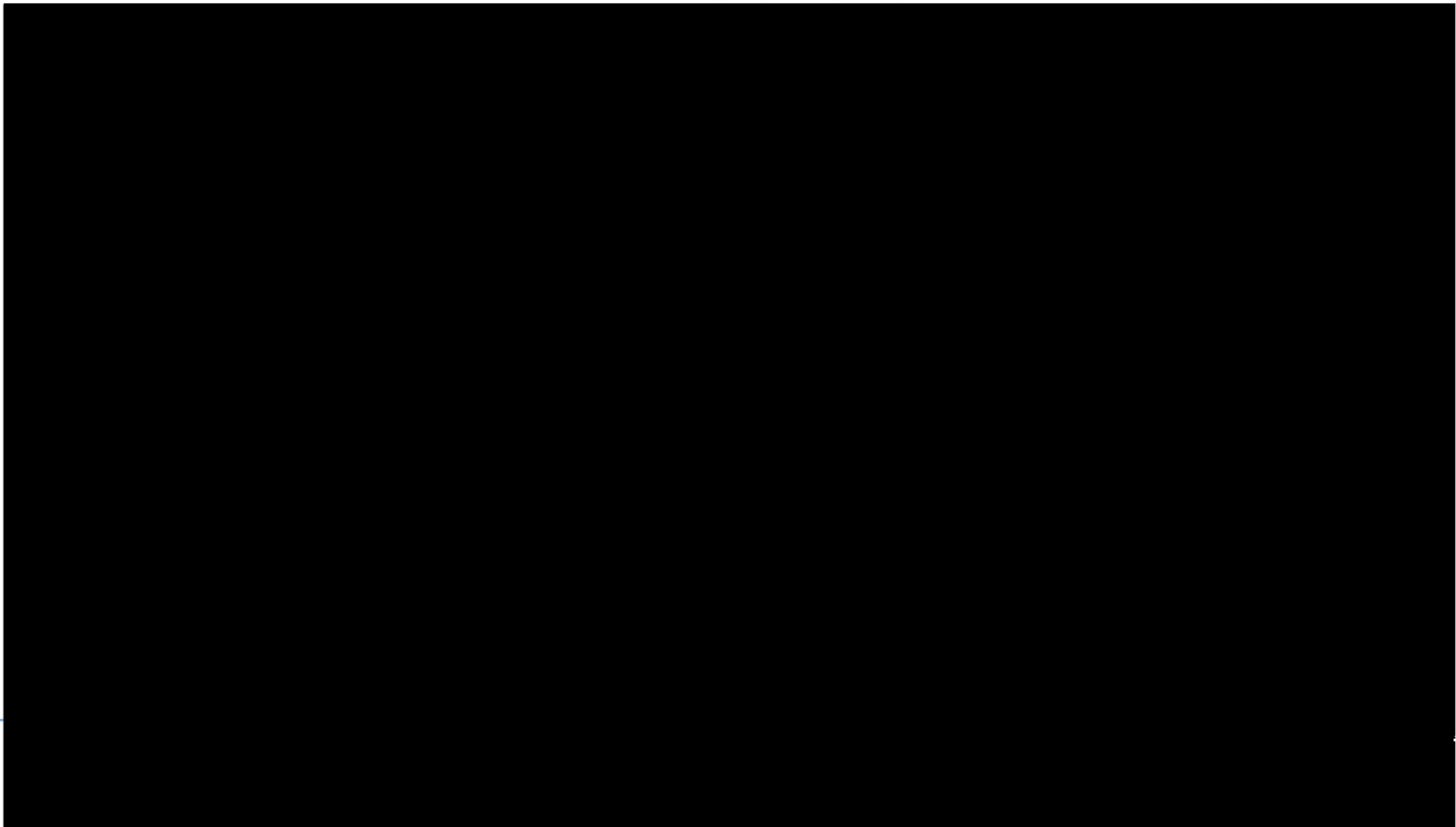


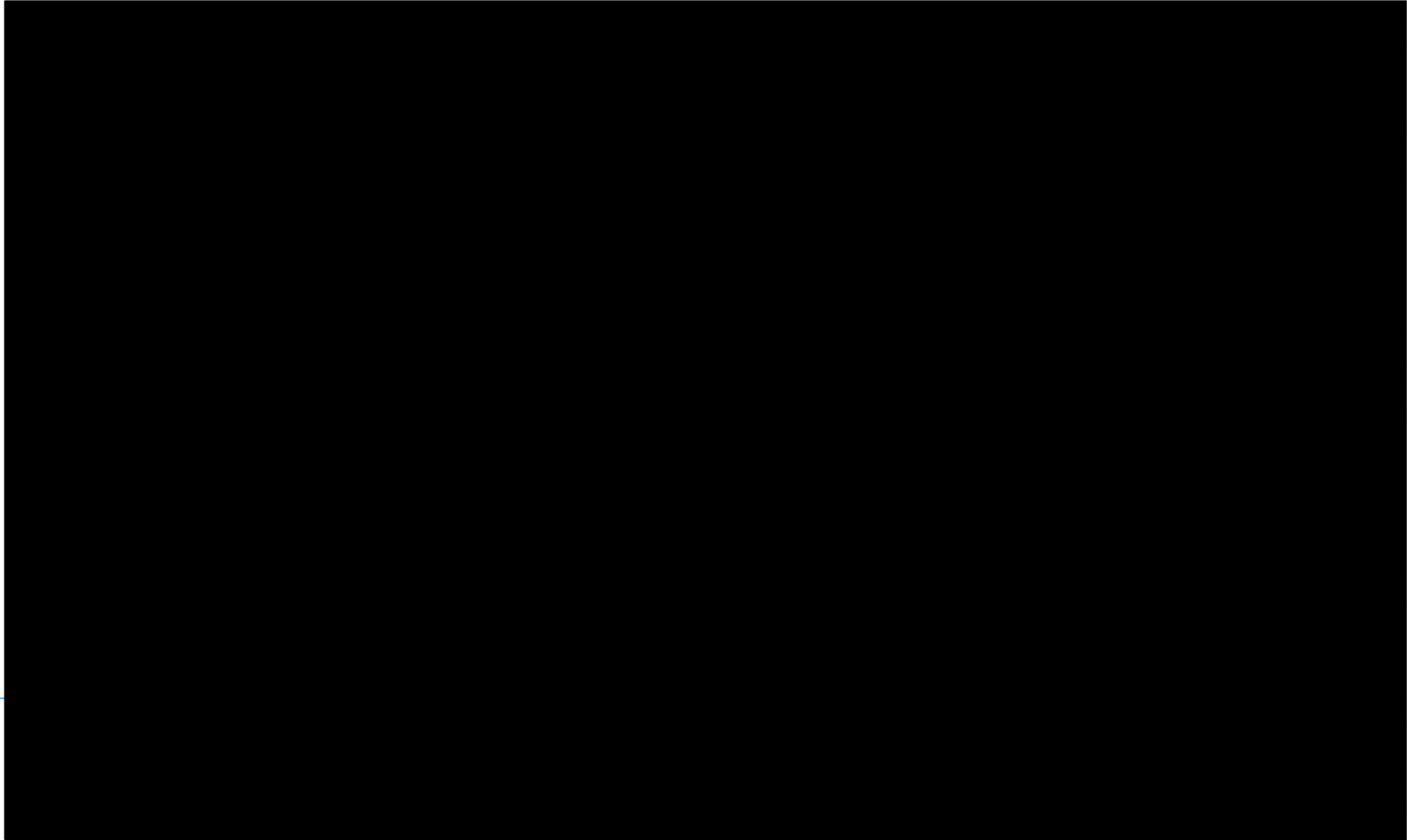




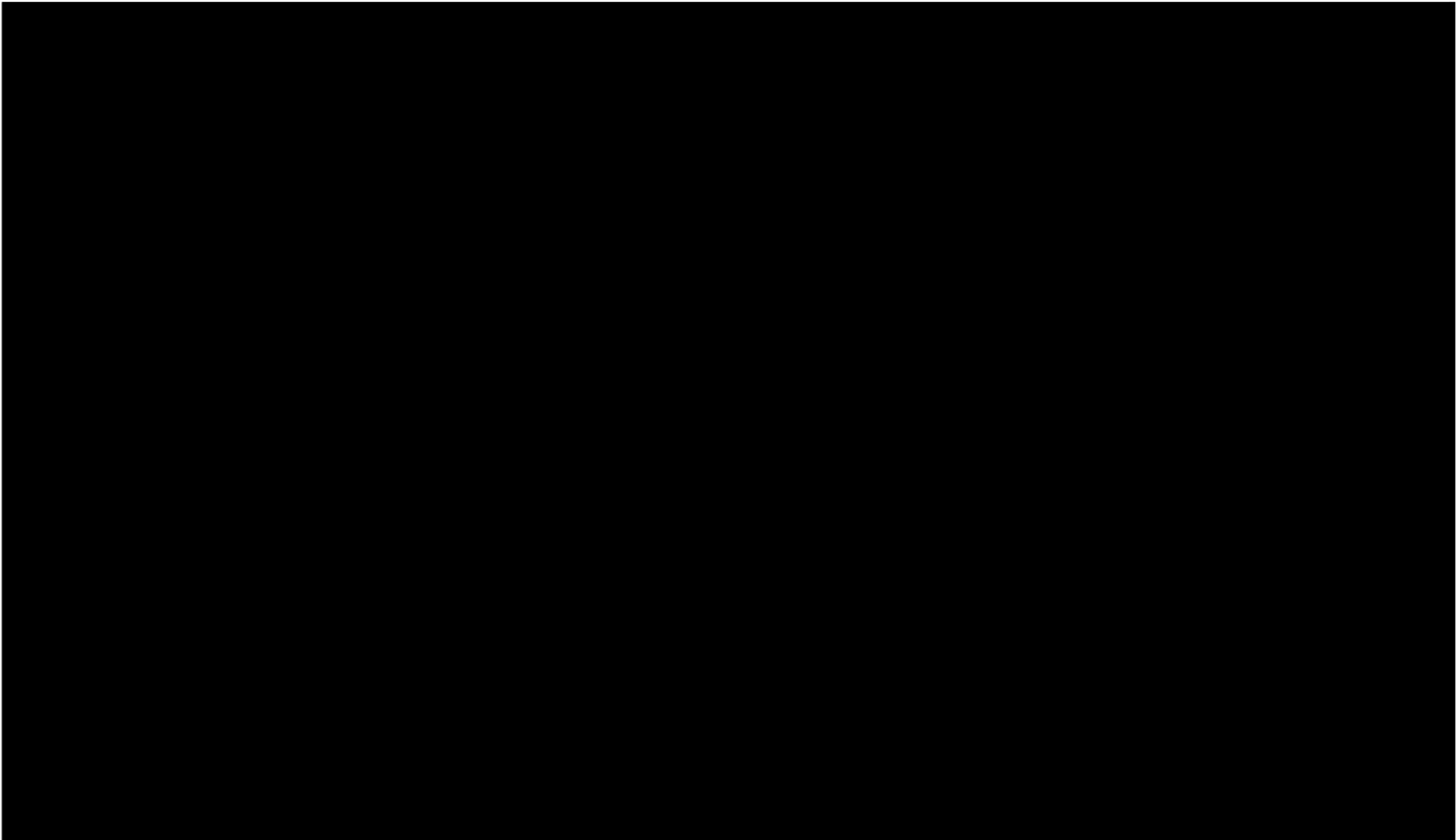


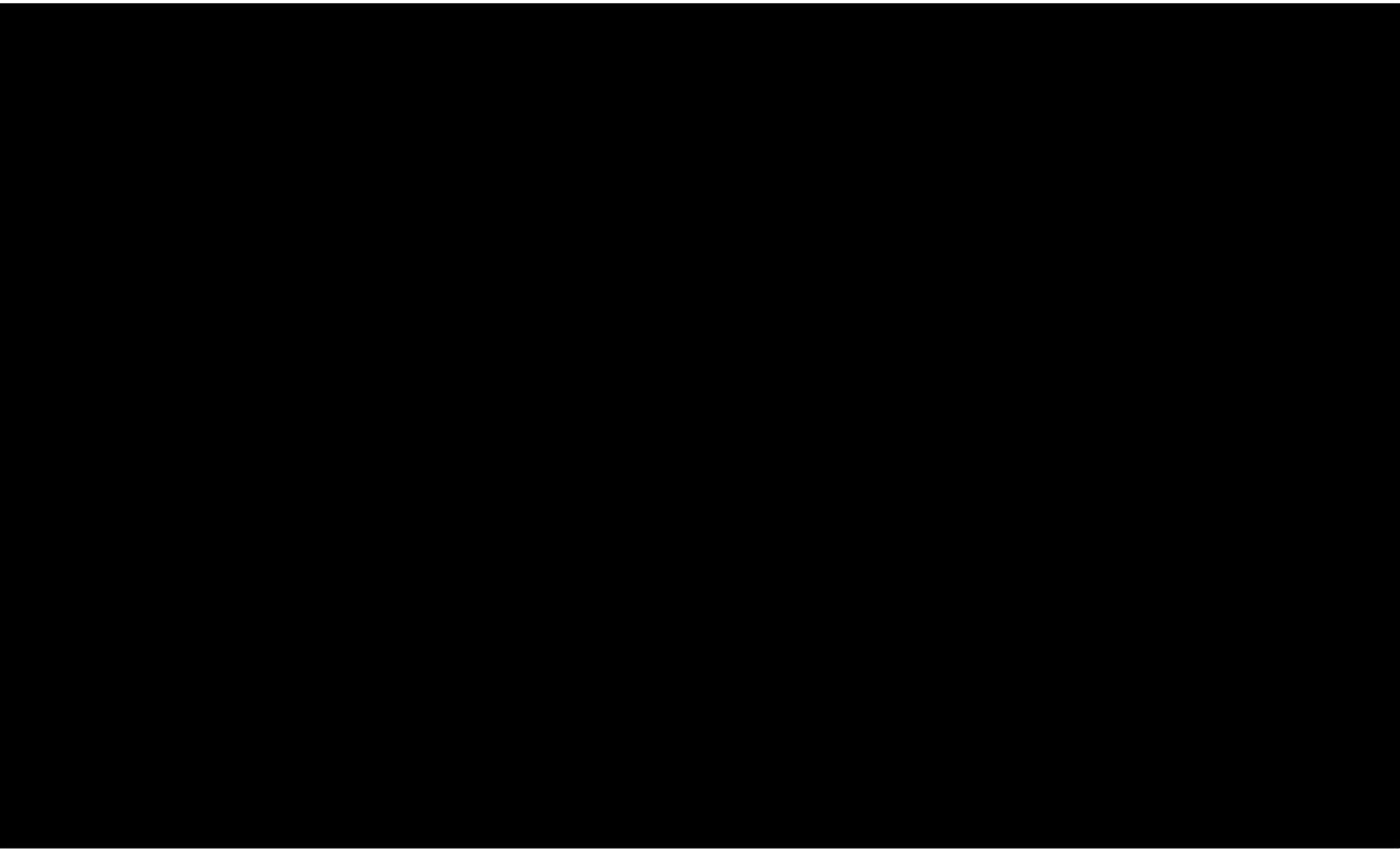


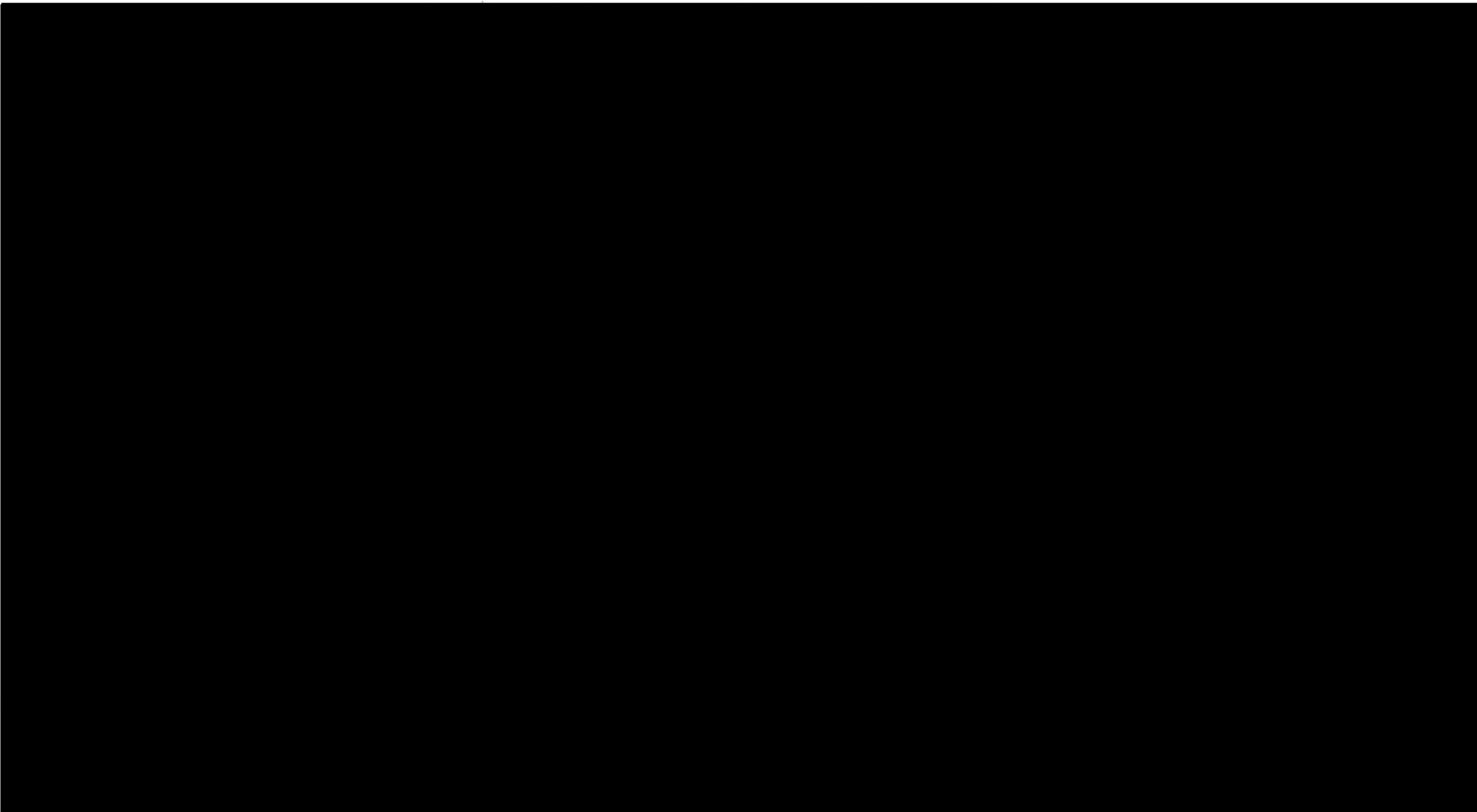






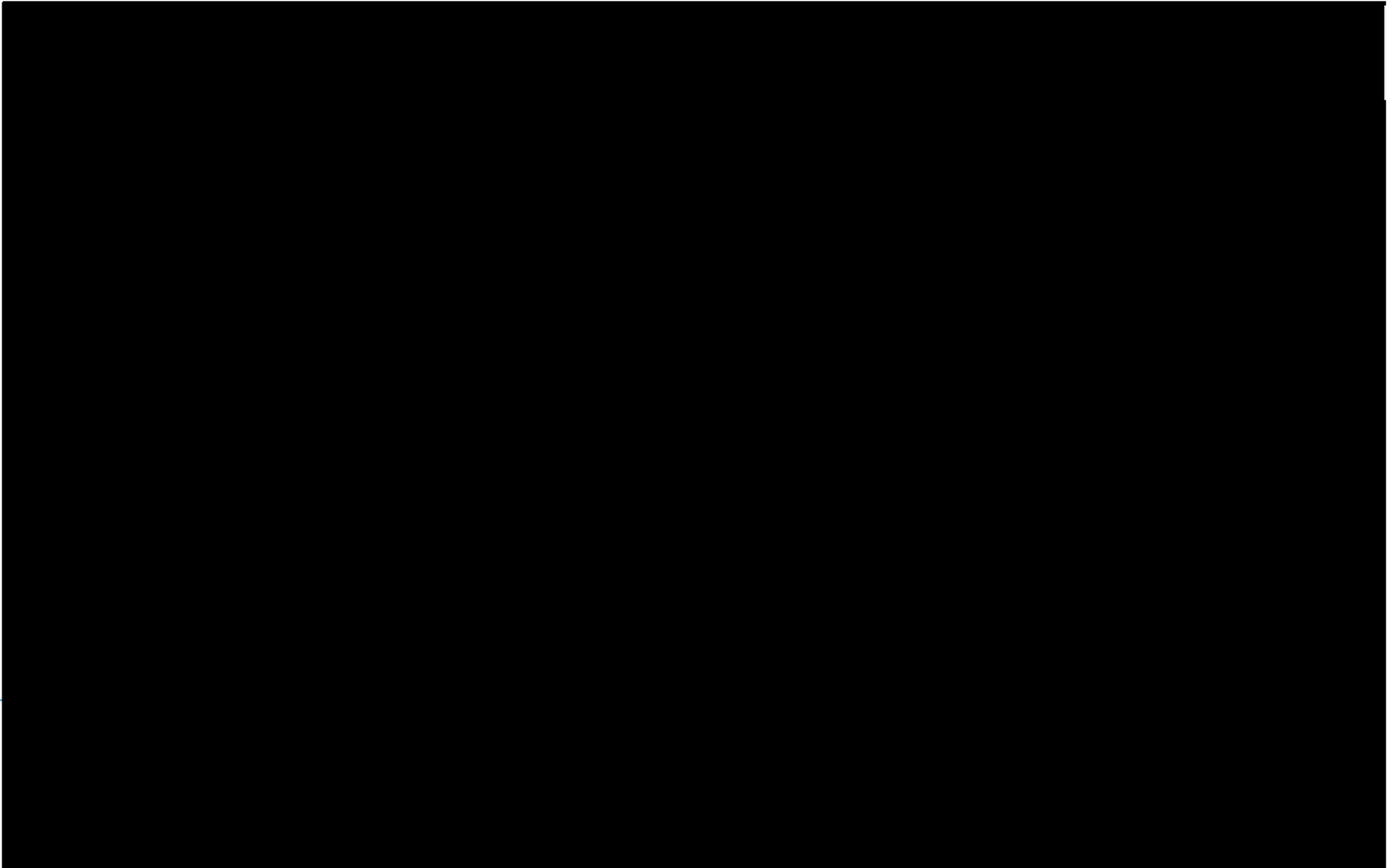




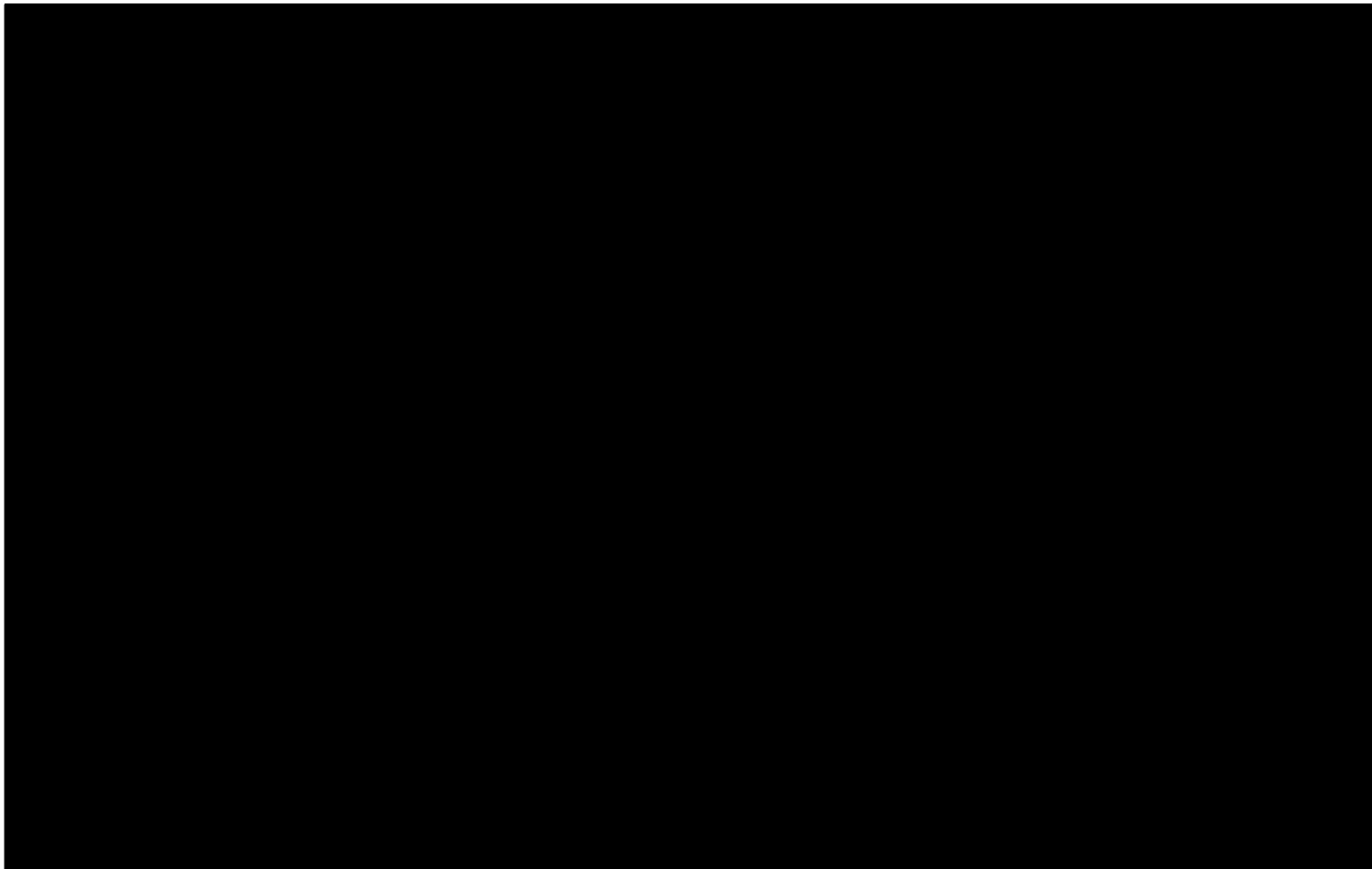


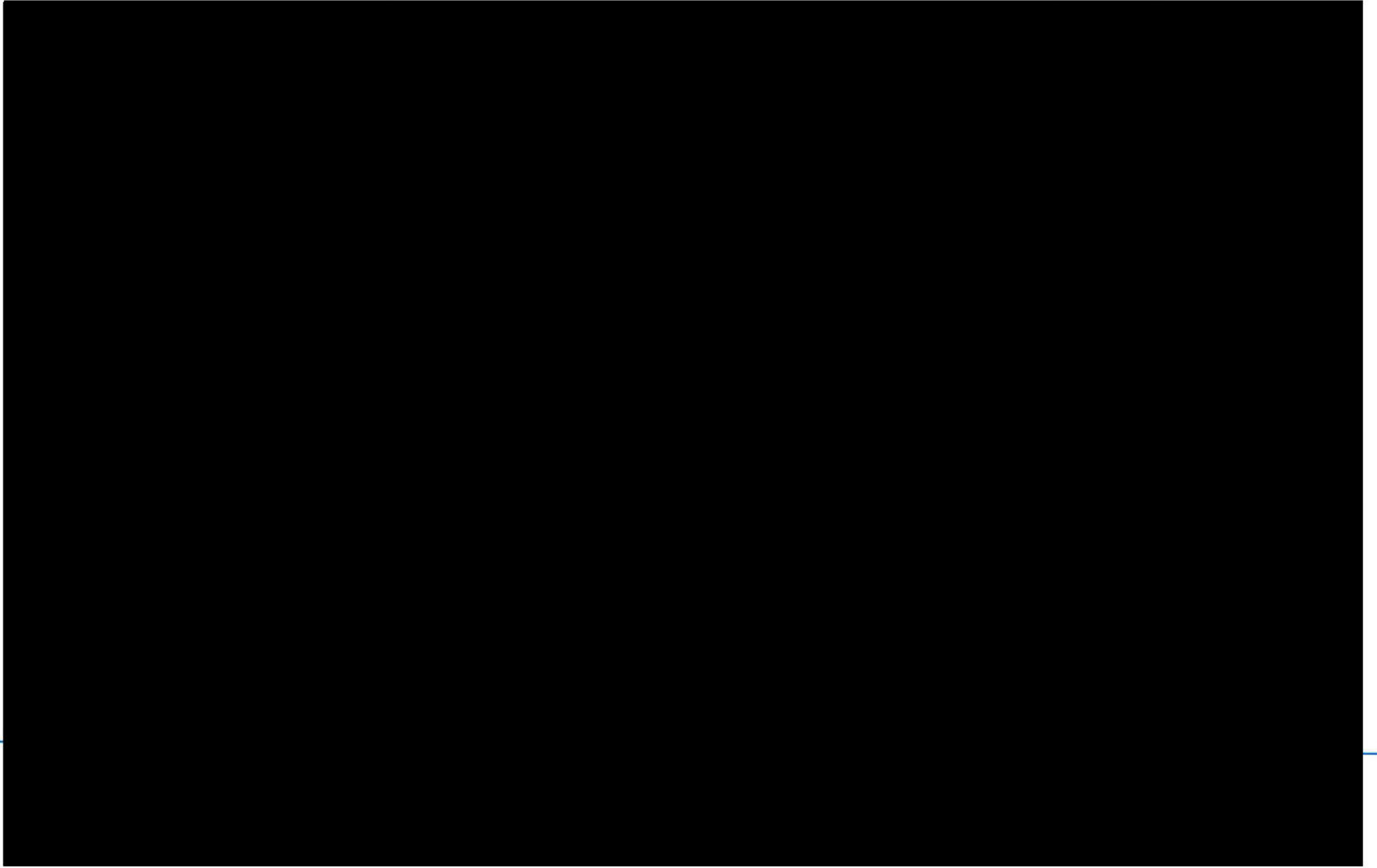


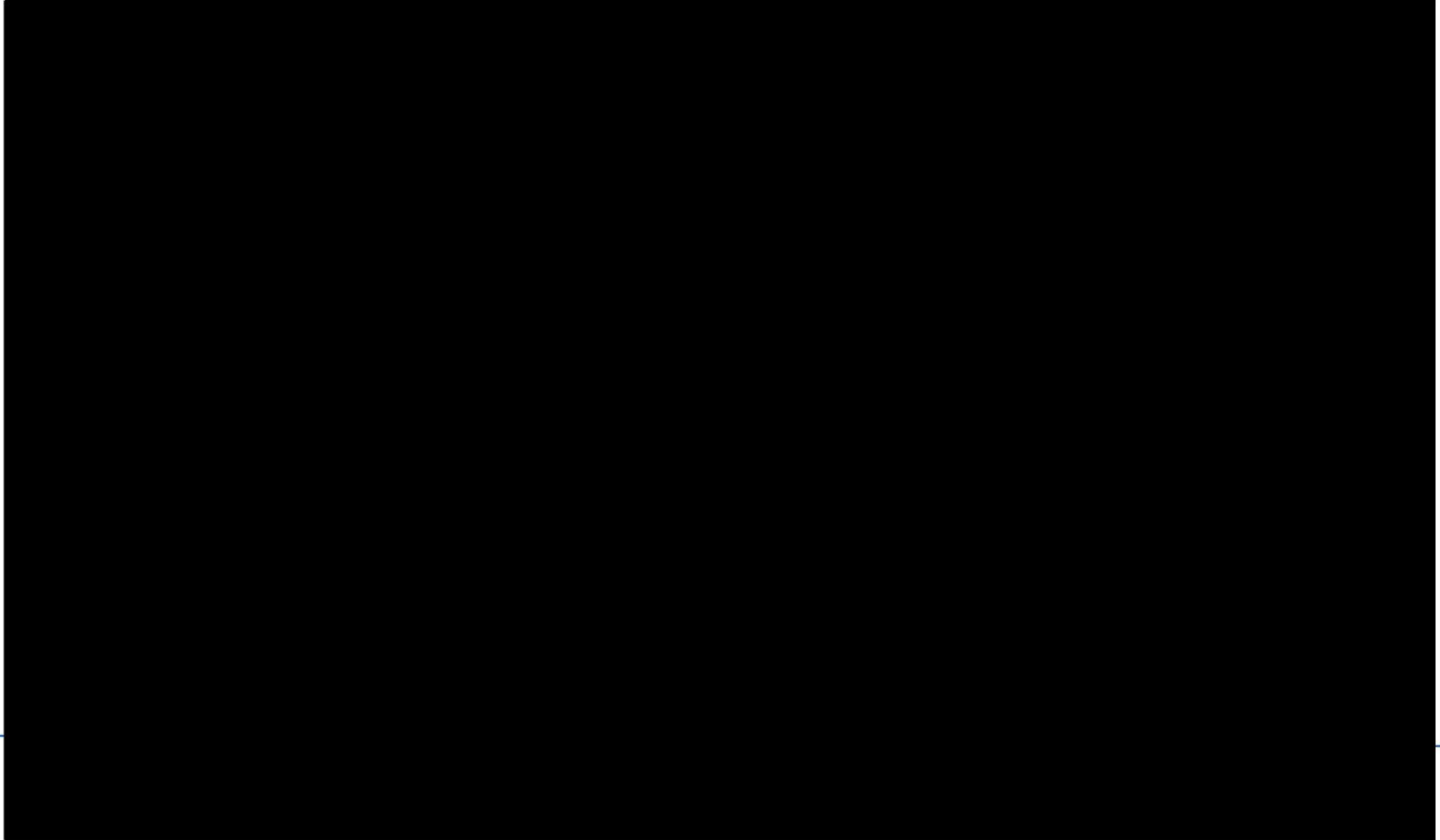


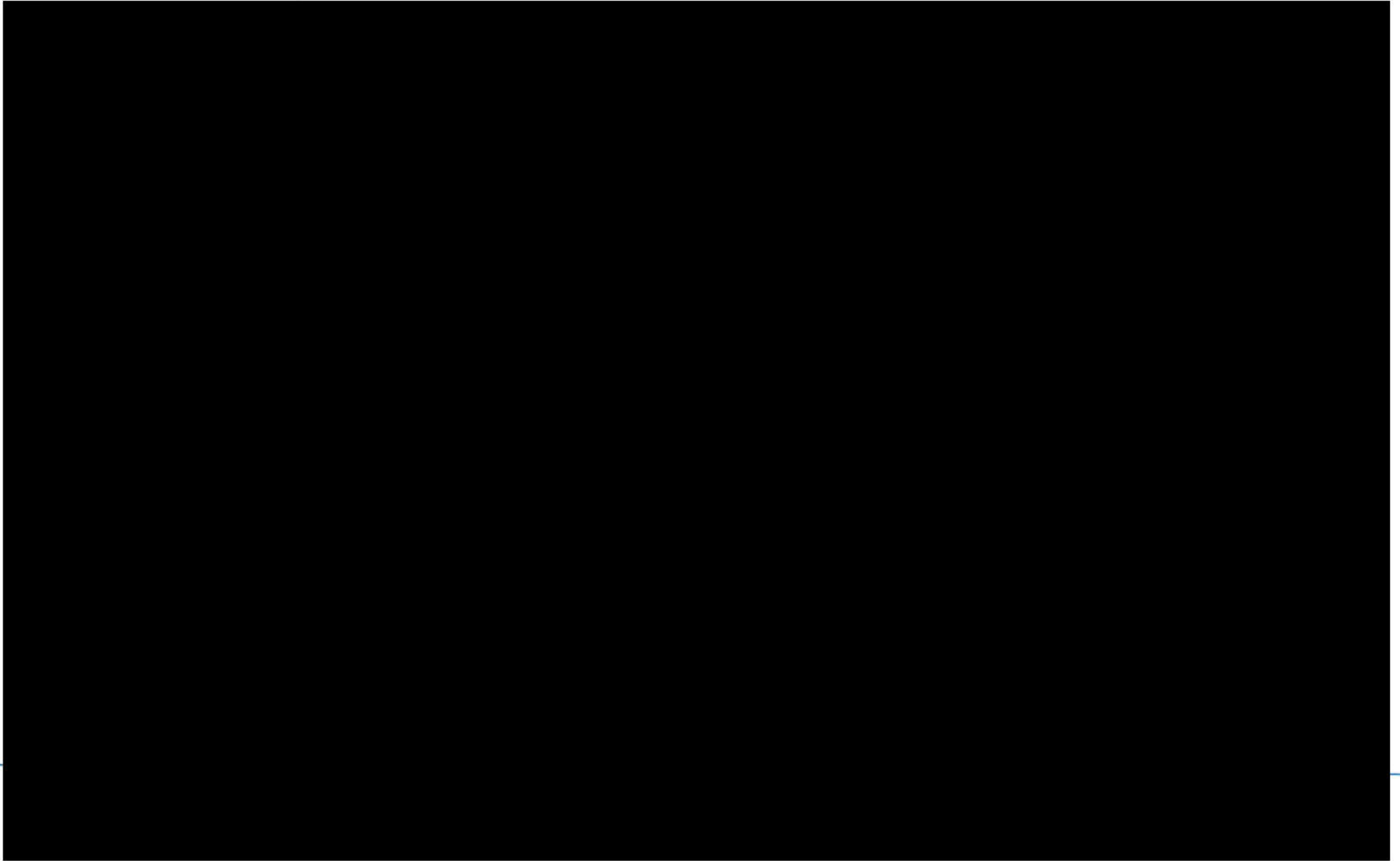


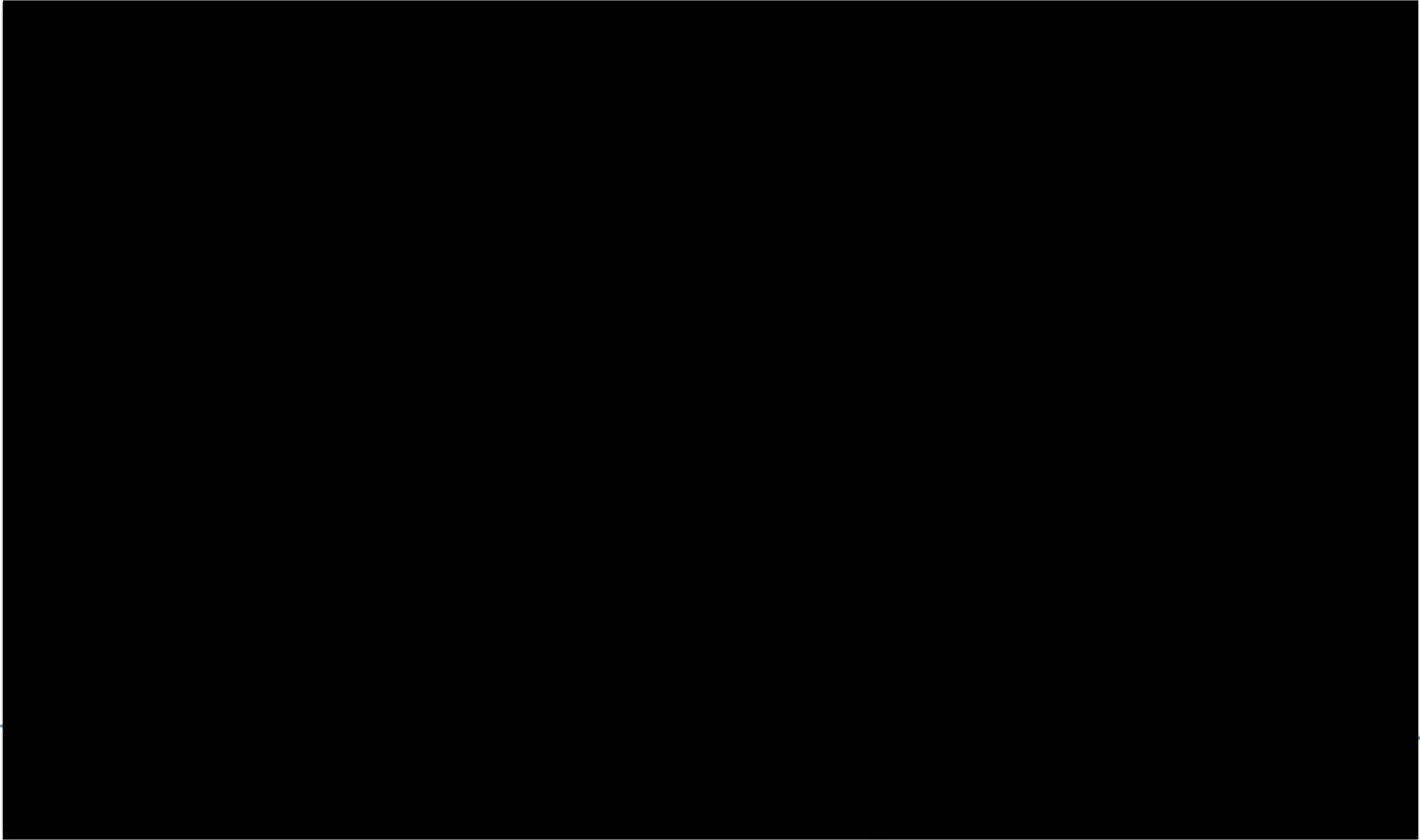


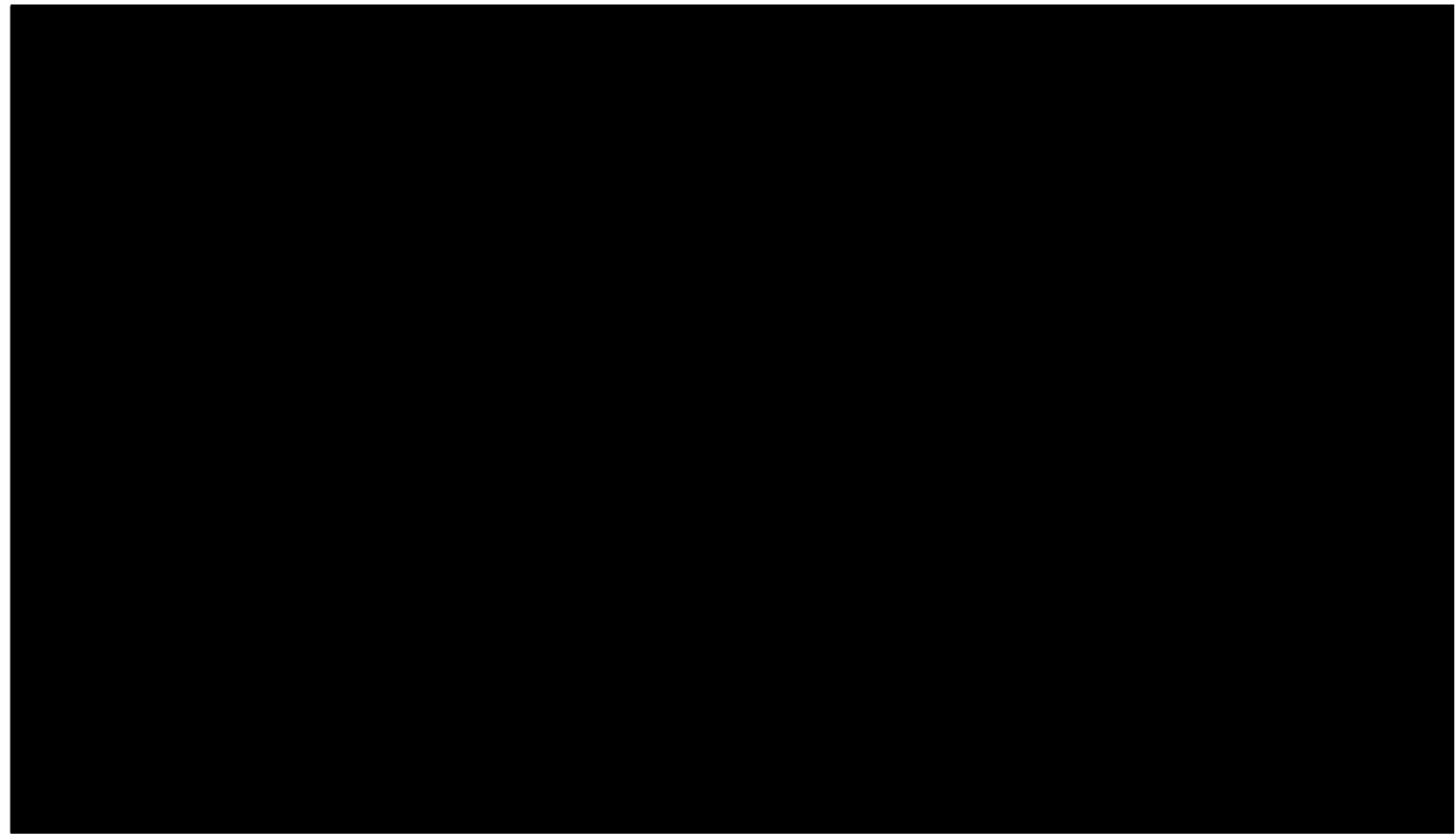


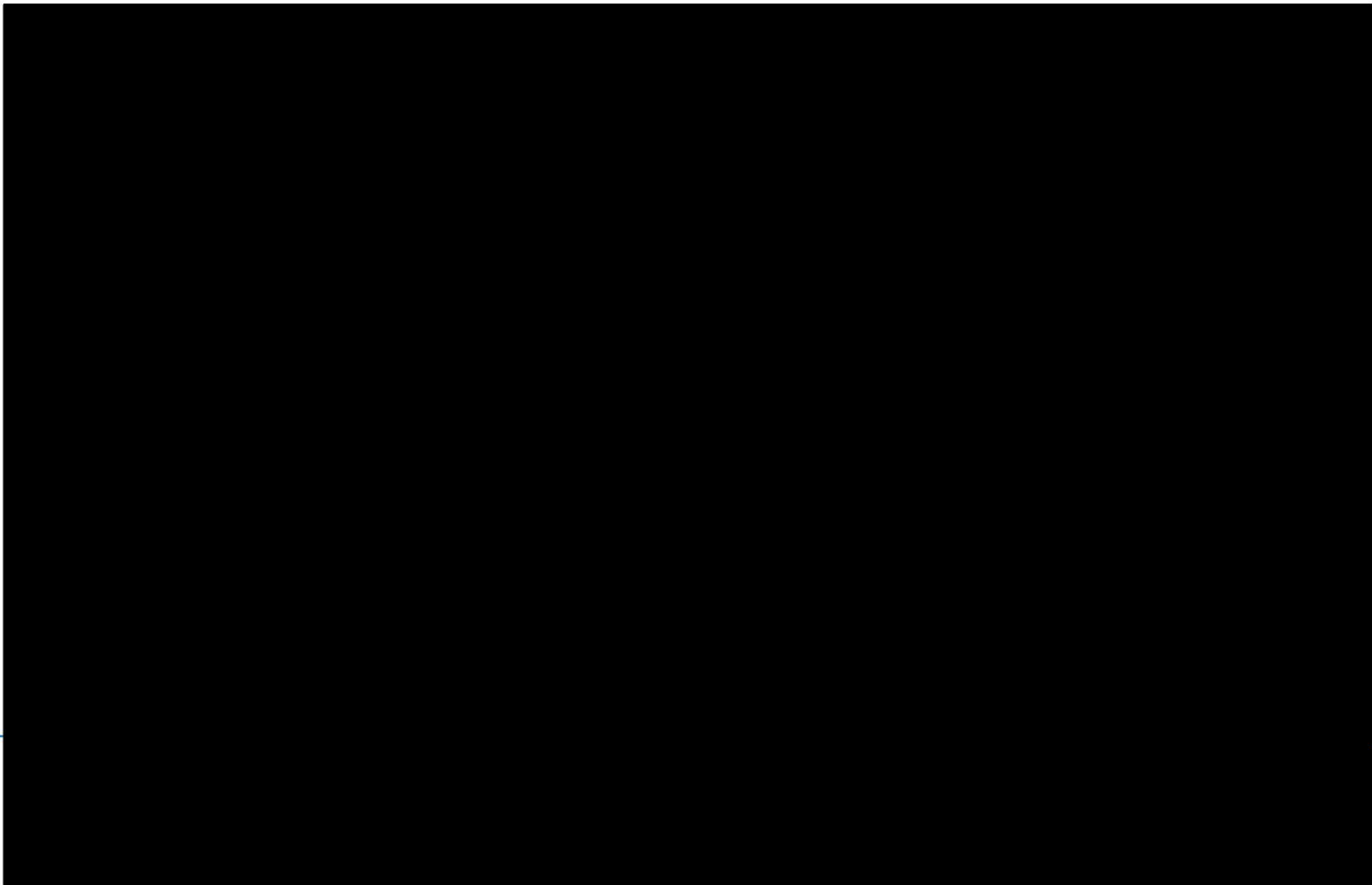


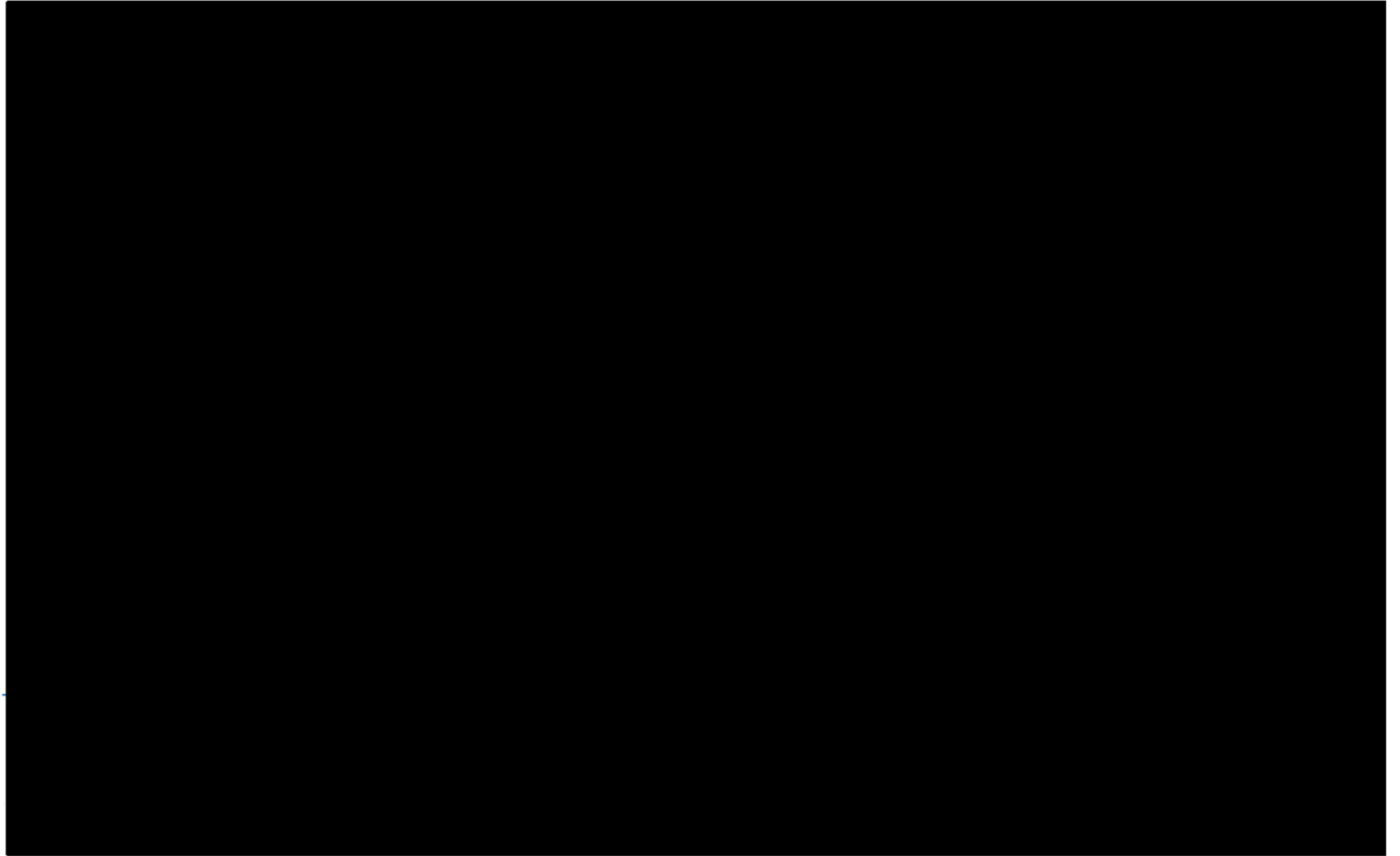


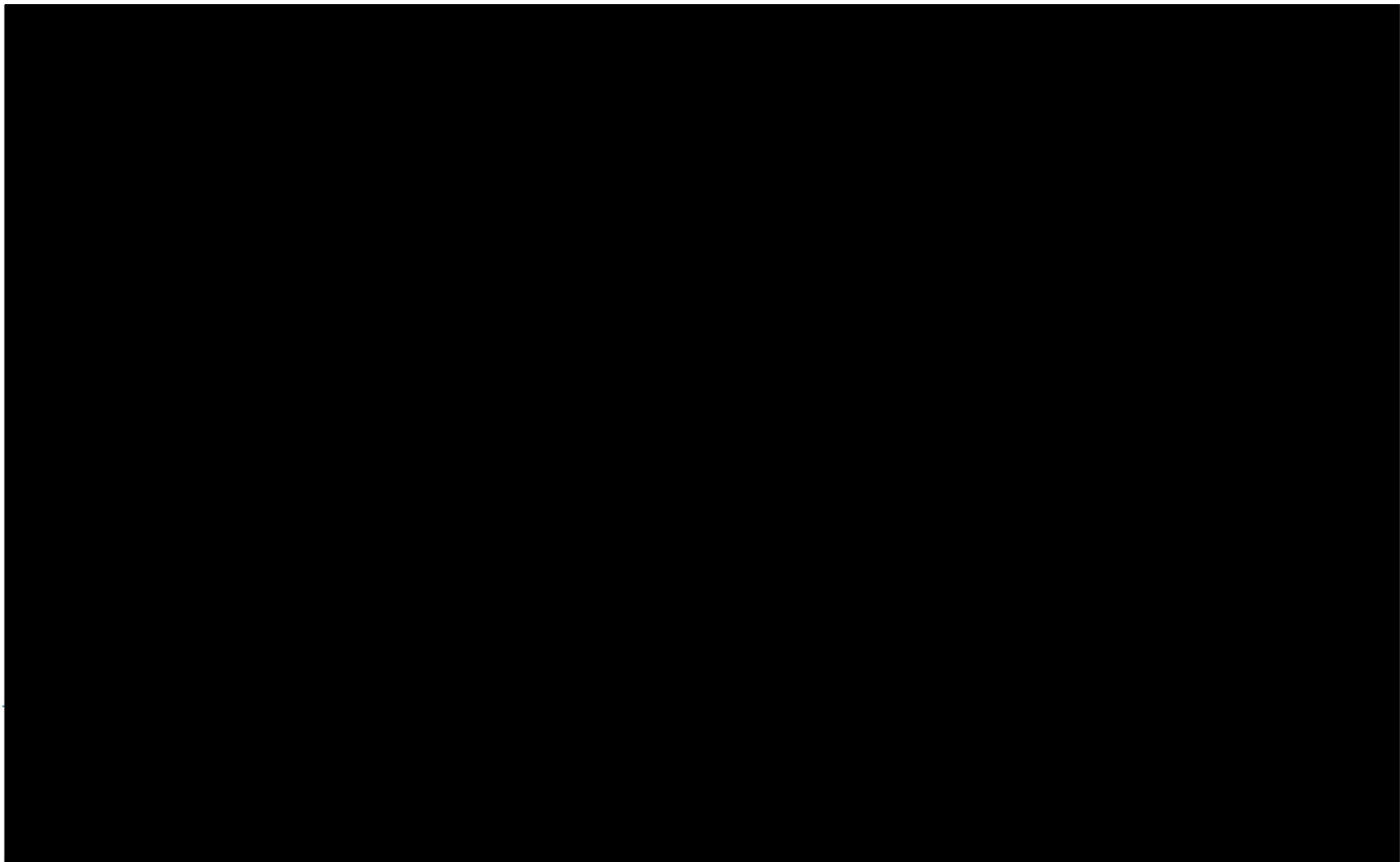


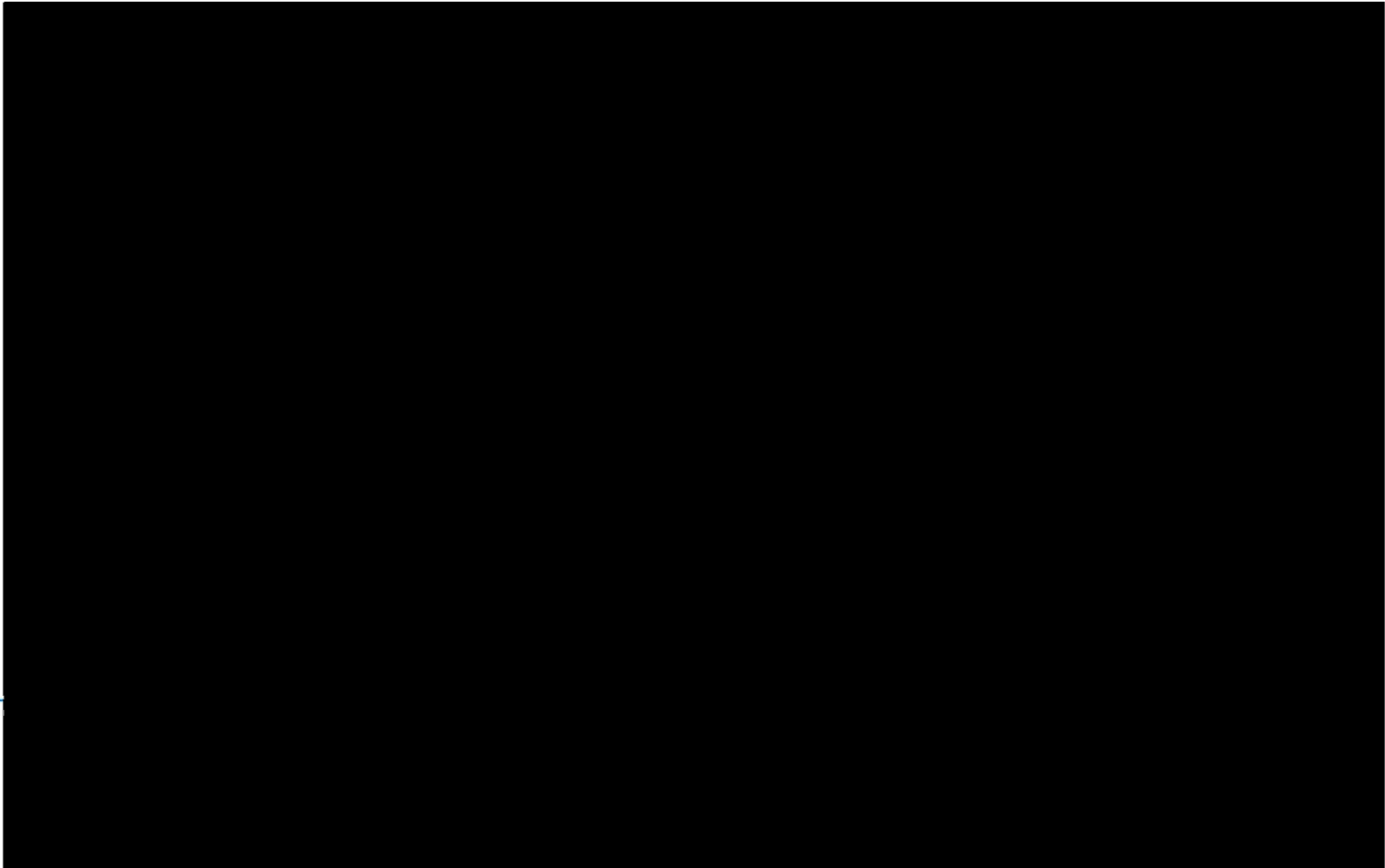


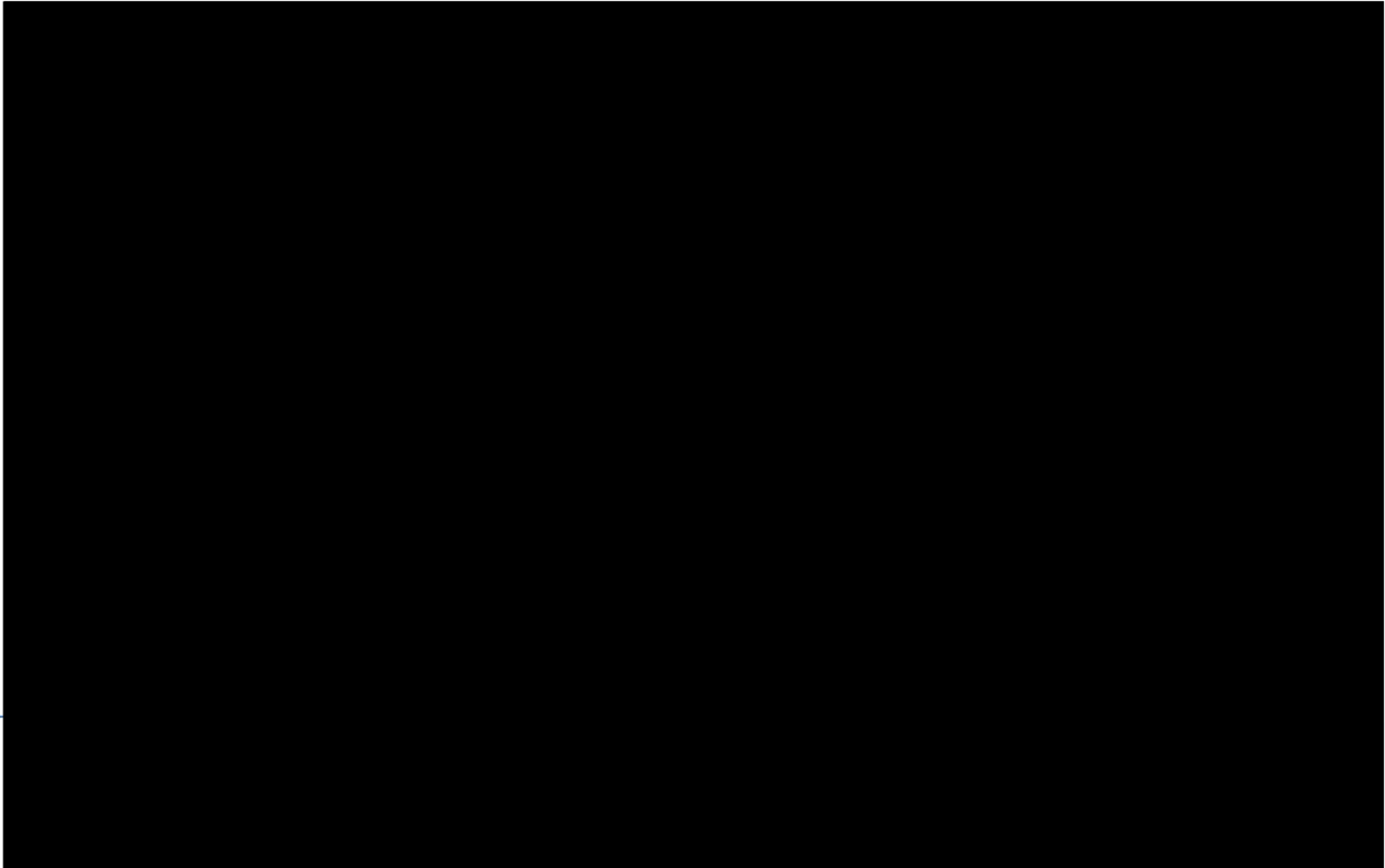


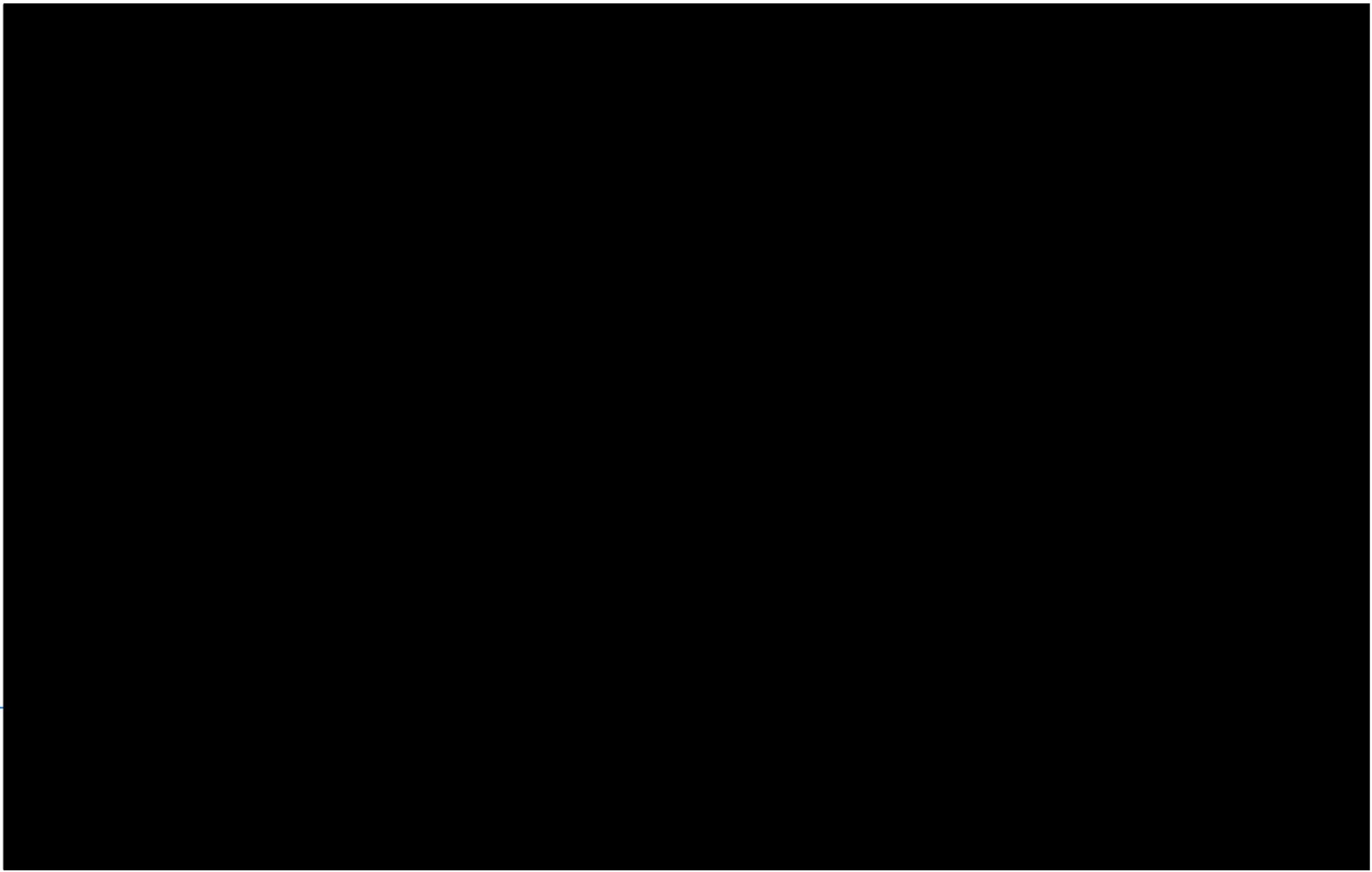


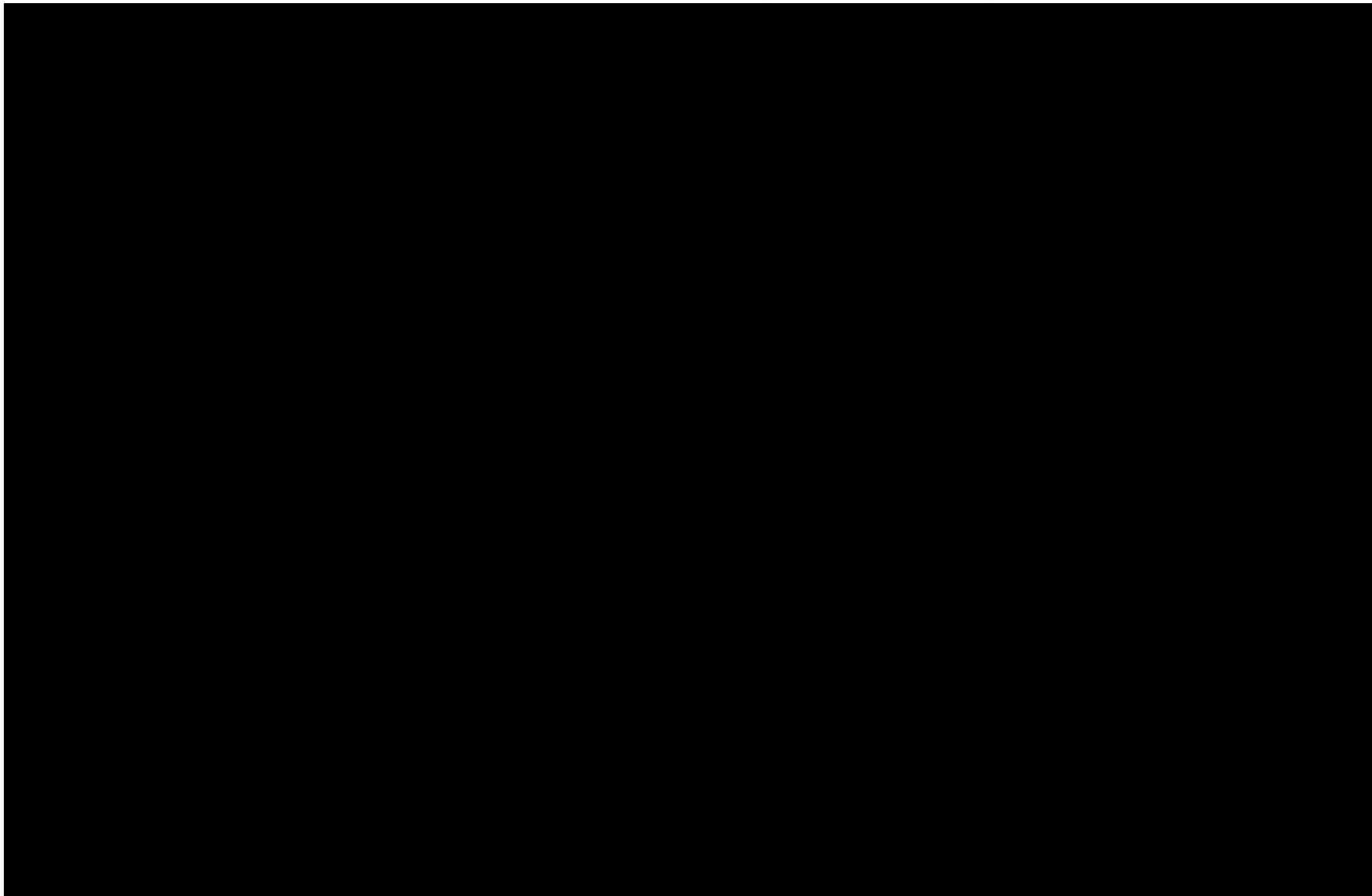


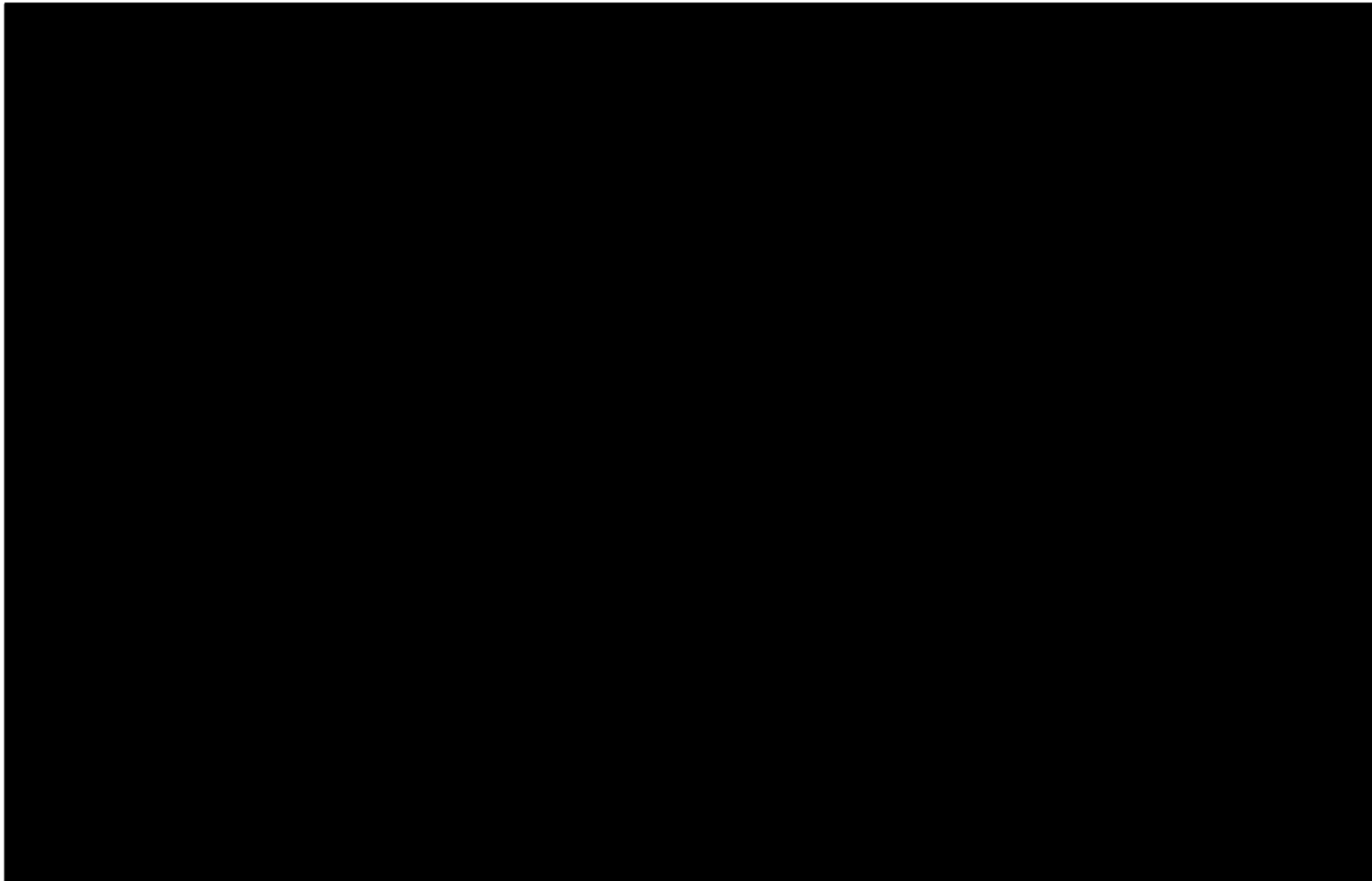




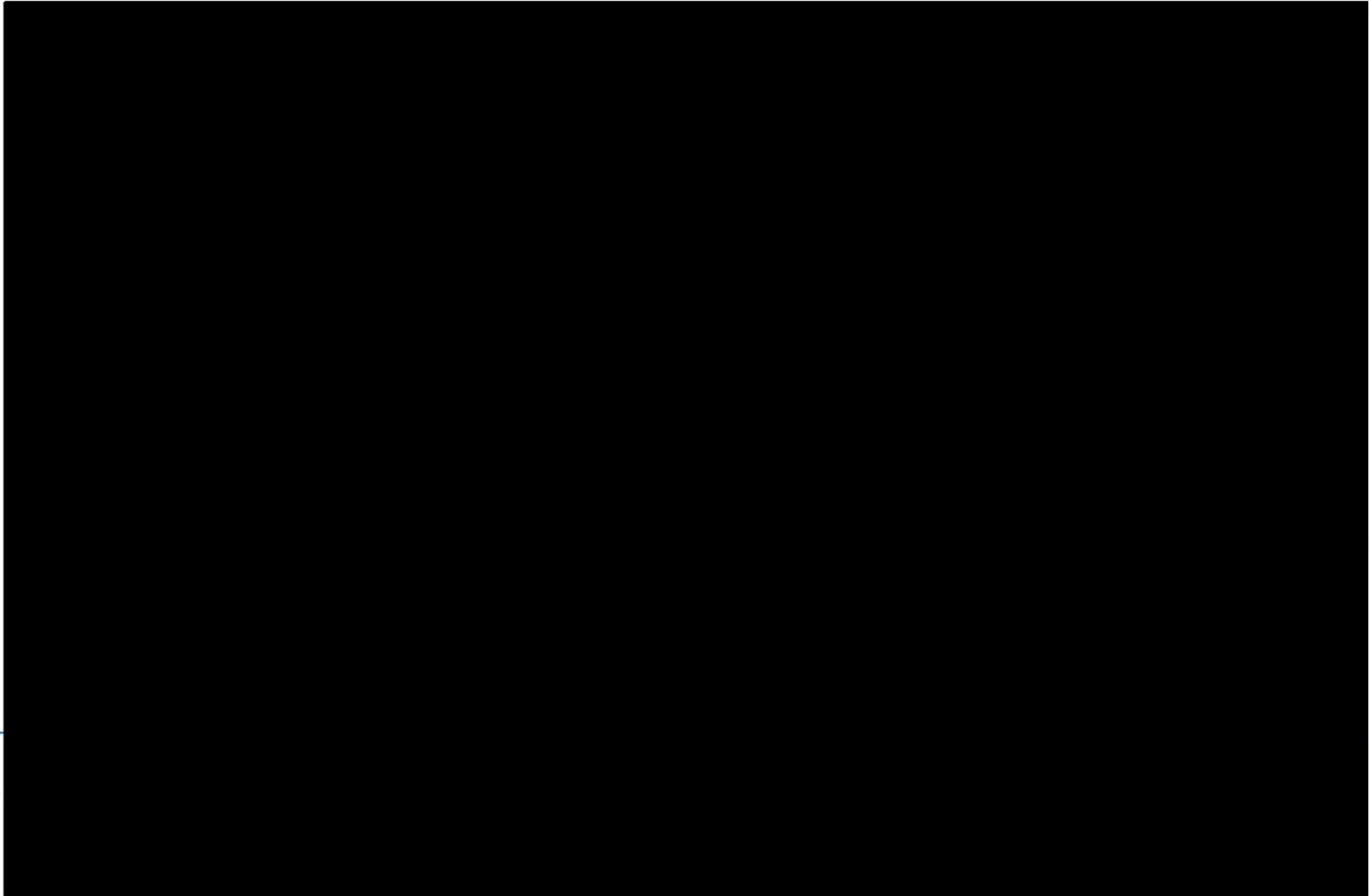


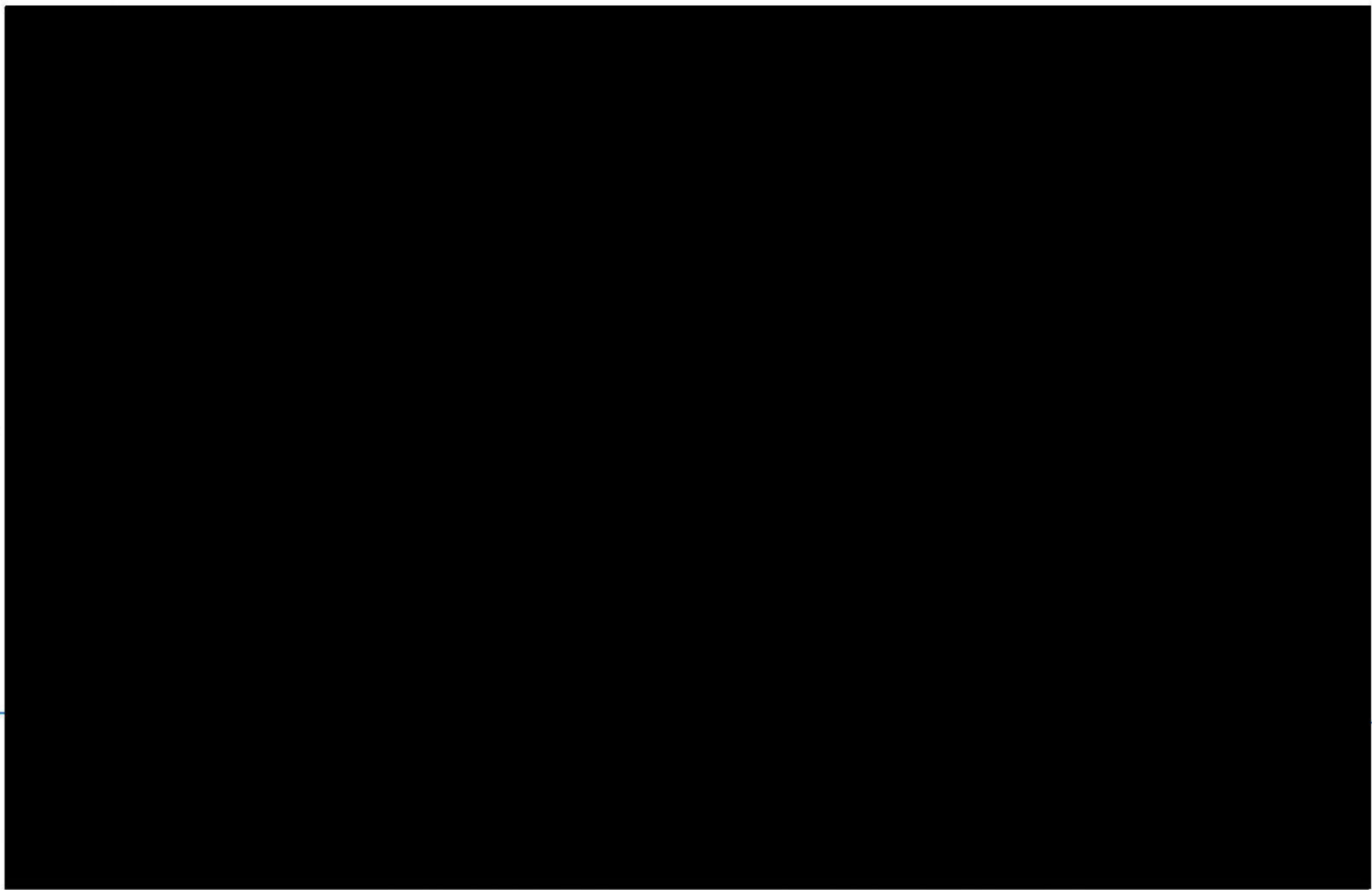


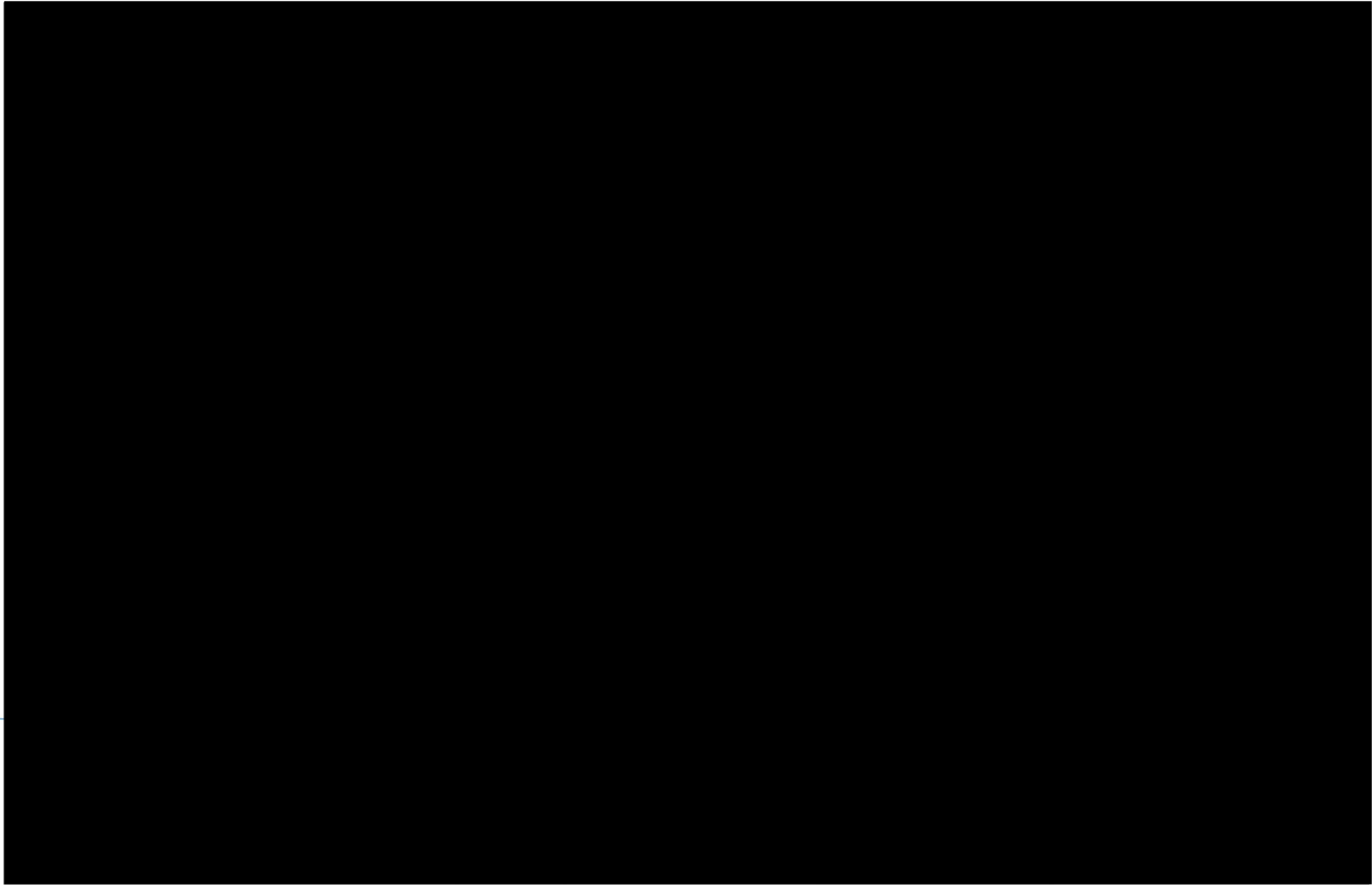




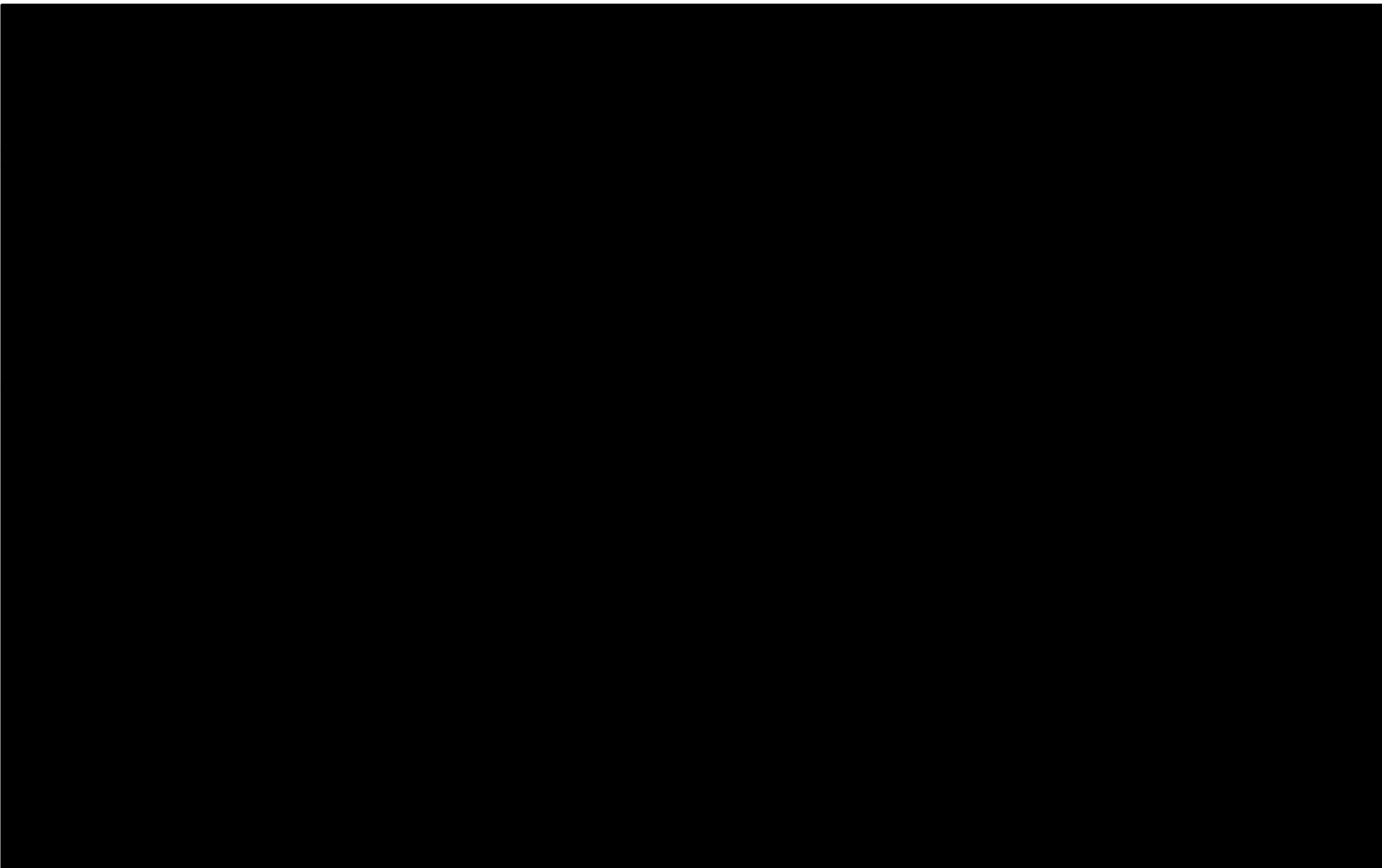


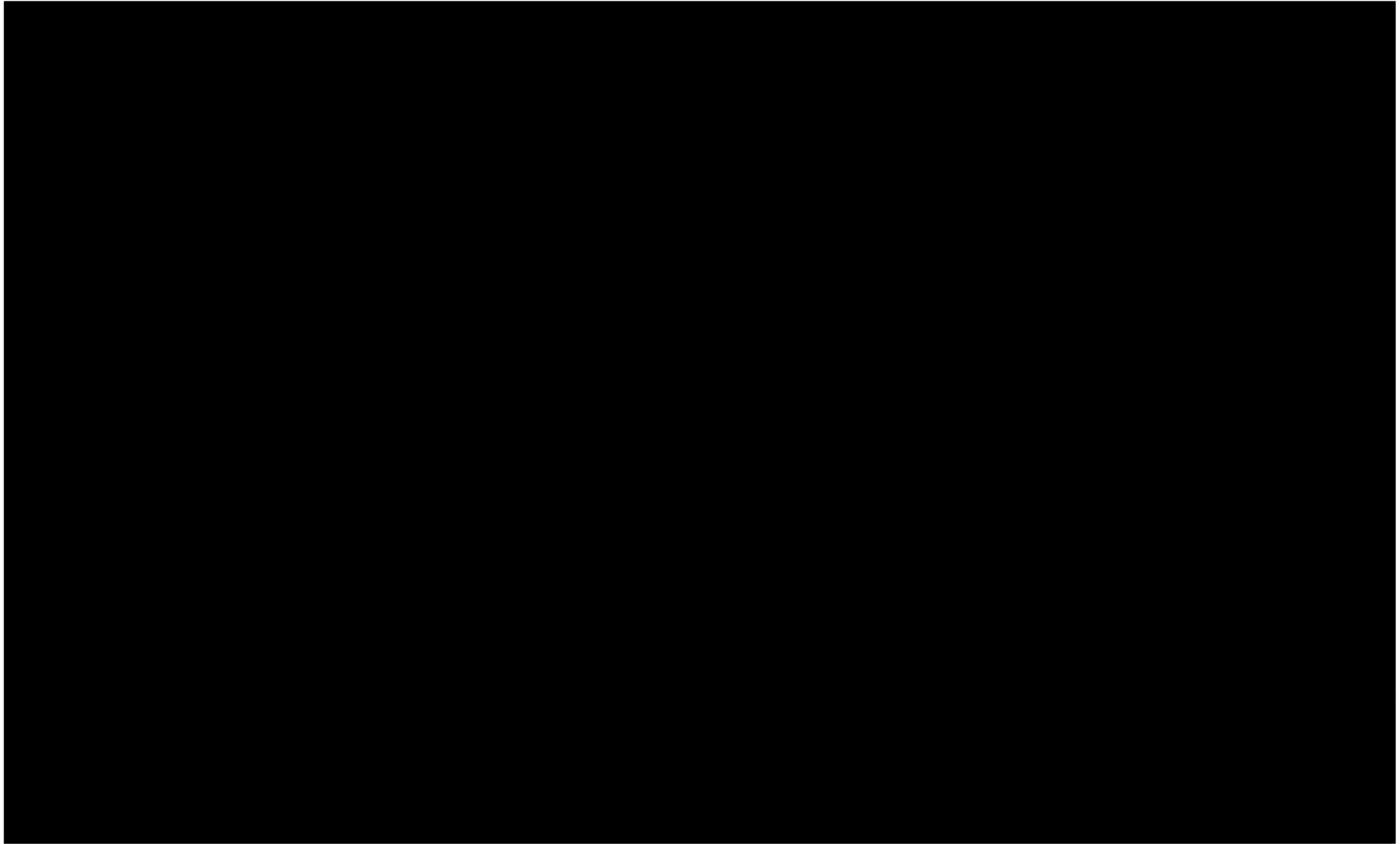


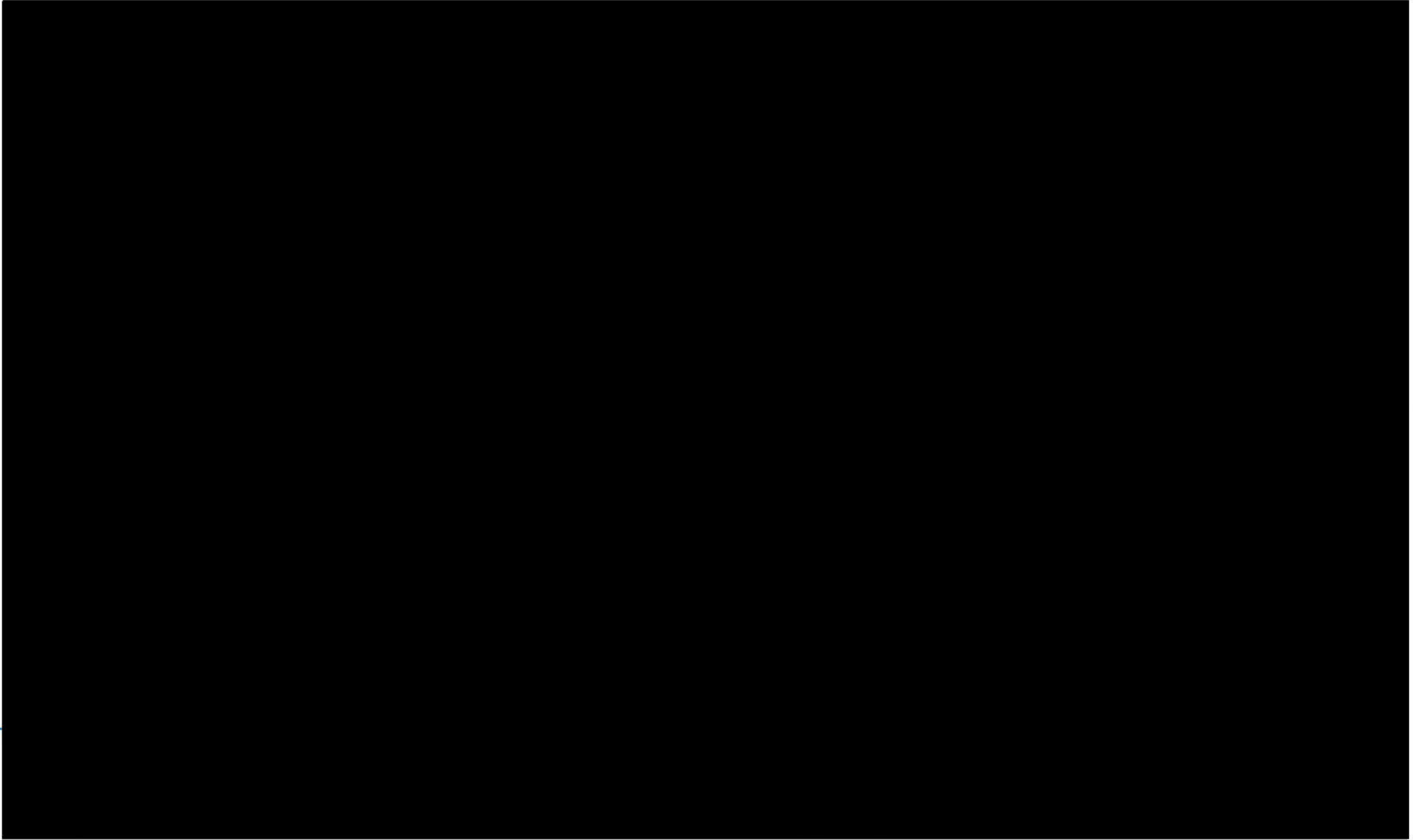






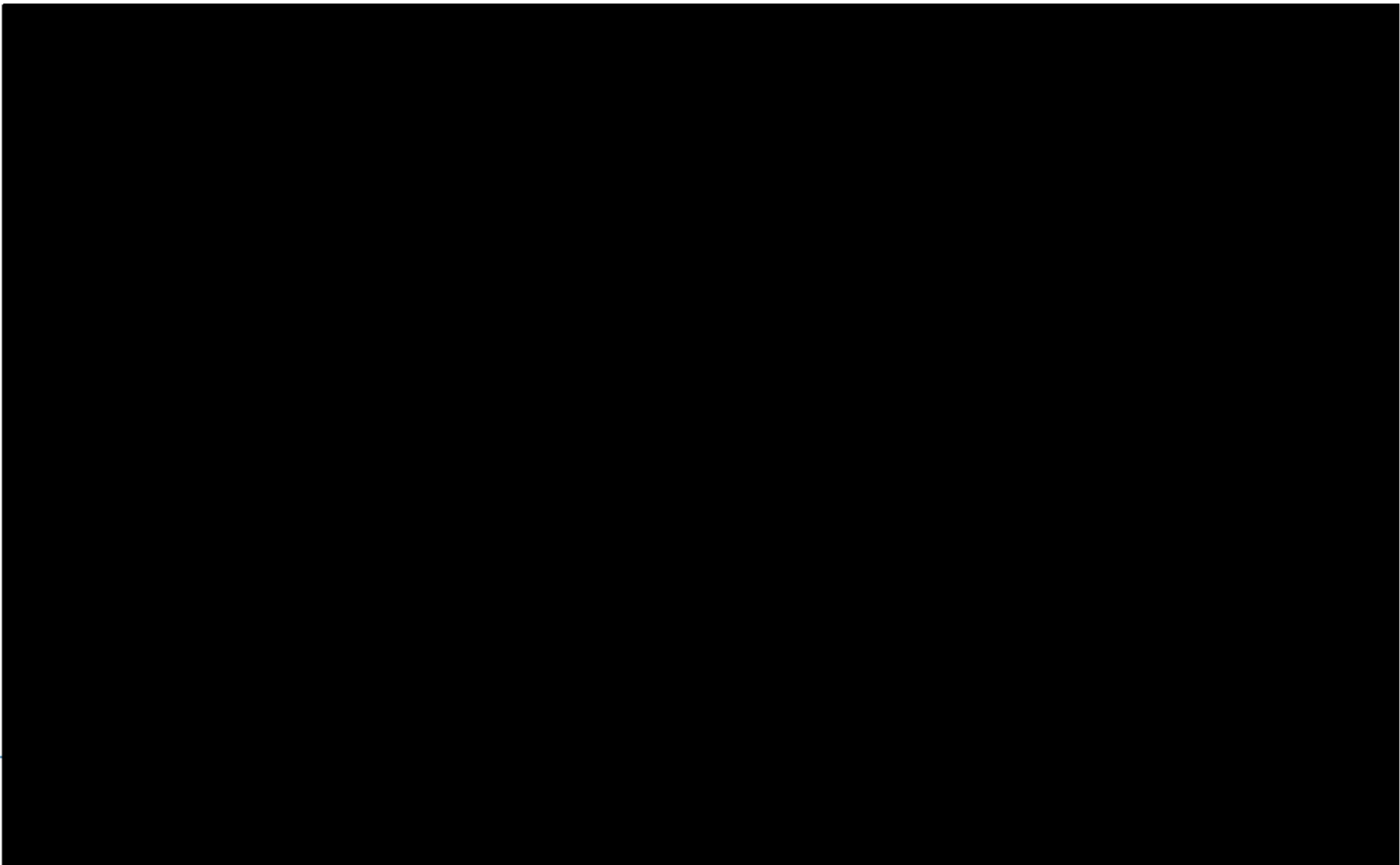


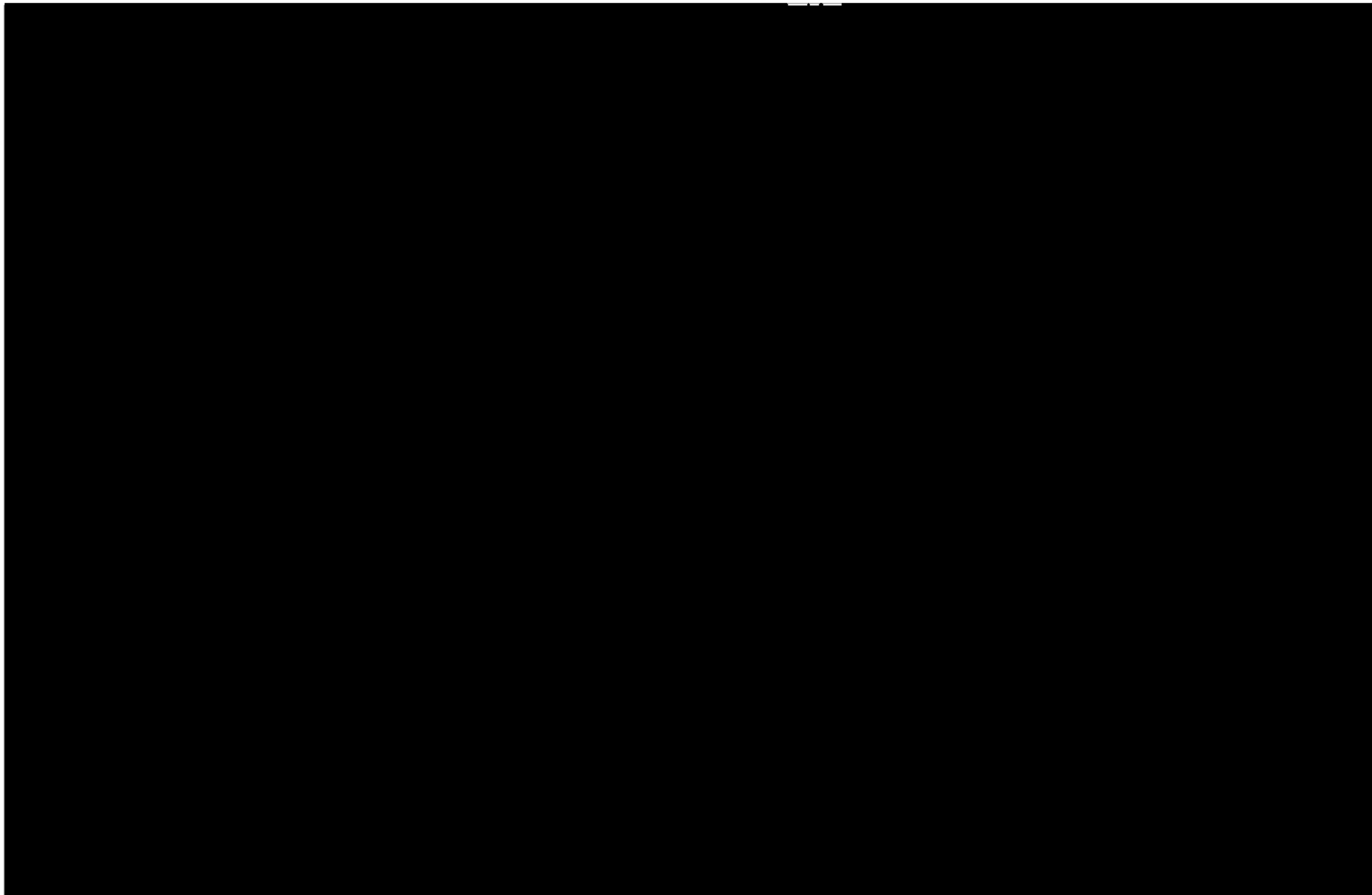


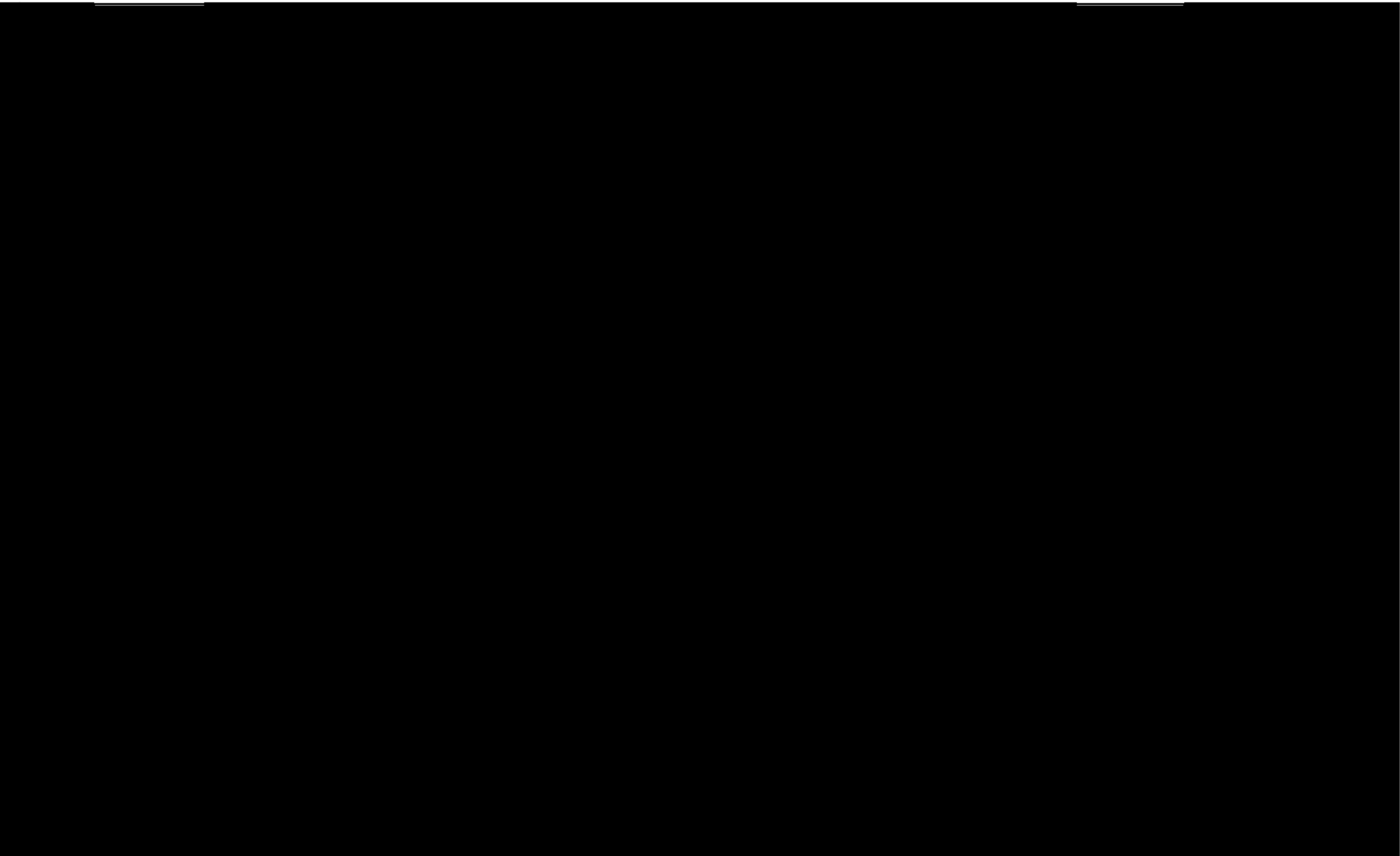


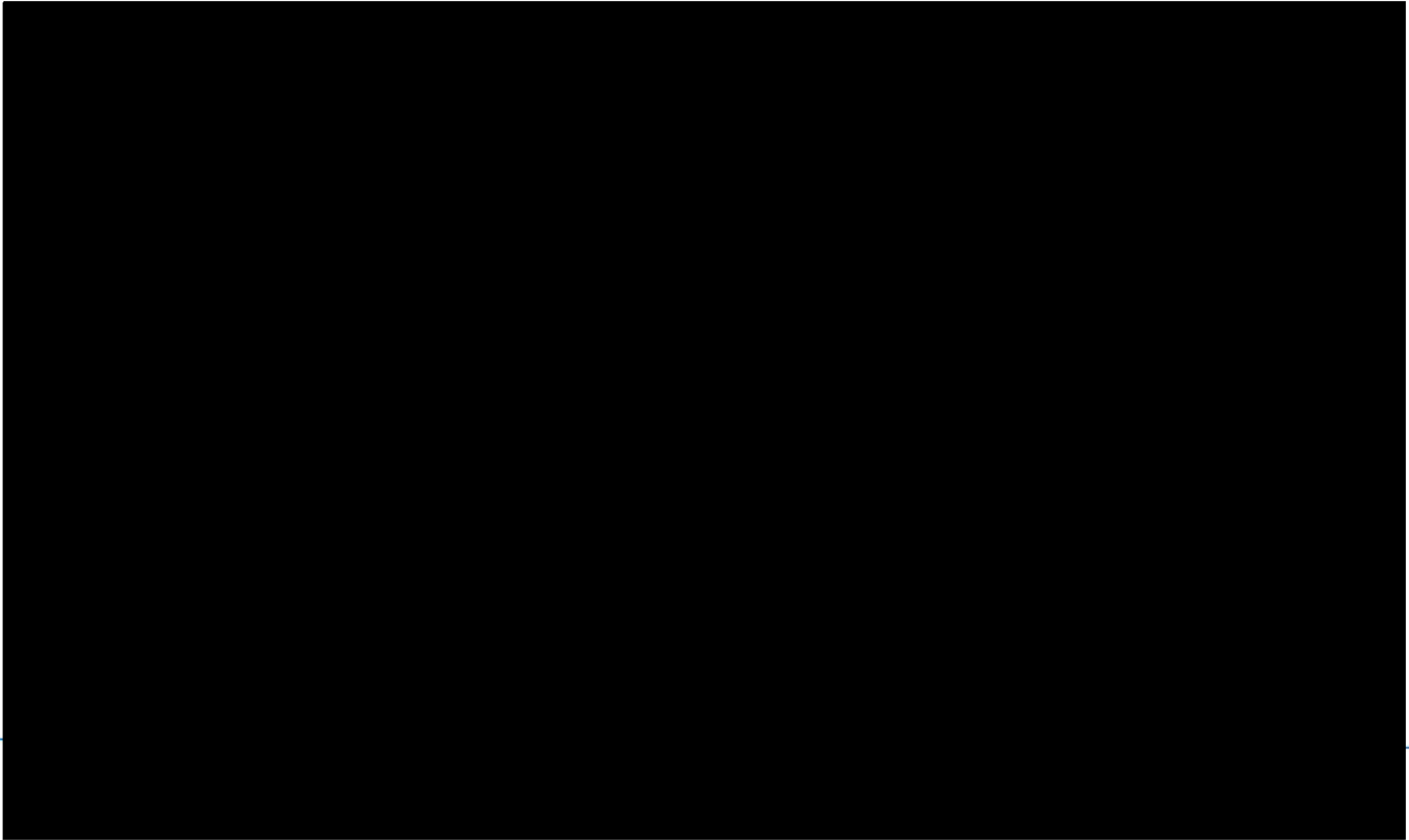


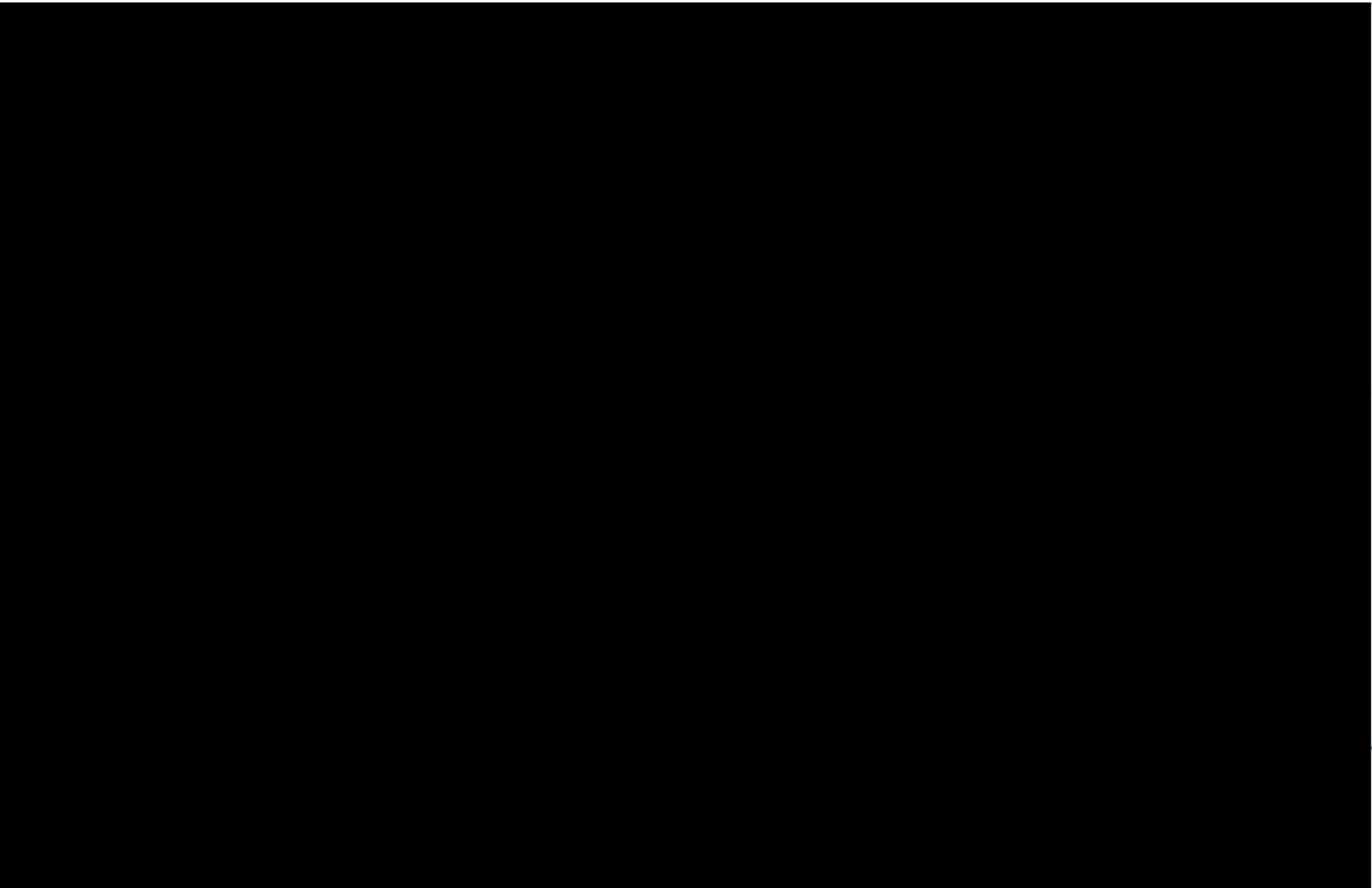














Attachment 3

Non-Disclosure Agreement (Mutual)



Non-disclosure agreement (mutual)

Parties	Macquarie University ABN 90 952 801 237 of Macquarie University 2109 (University). KPMG ABN 51 194 660 183 of 300 Barangaroo Avenue, Sydney NSW 2000
Agreement	The parties to this agreement wish to share information, including Confidential Information, for the Purpose and agree to share that information on the terms set out below and in the attached document headed 'General Terms'. These General Terms form part of this agreement.

Details	
Defined Term	Meaning
Commencement Date	10/03/2023
Purpose (clause 2)	The purpose for which this disclosure of confidential information is made is to respond and discuss the [REDACTED] and negotiate the resulting contract if successful in the bid.
Term (clause 2)	12 months
Special Terms	This agreement is subject to the following special terms. If no special terms insert 'Not applicable'.



MACQUARIE
University

Signed on behalf of **MACQUARIE UNIVERSITY** by its authorised officer:

Signature of authorised officer

Natalie Budovsky

Name of authorised officer

15/03/23

Date

Chief Procurement Officer

Position of authorised officer

Signed on behalf of **KPMG** by its authorised officer:

Signature of authorised officer

David Cummins

Name of authorised officer

14 March 2023

Date

Partner

Position of authorised officer



General Terms

1. Interpretation

1.1 Definitions

The following definitions apply in this agreement.

Commencement Date means the date specified in the Details or, if no date is specified in the Details, the date on which this agreement became executed by all parties.

Confidential Information means information in any form or medium that is not Excluded Information and that:

- (a) relates to the past, present or future operations or affairs of the Disclosing Party or its controlled entities and:
 - (i) the Disclosing Party makes the Receiving Party aware is considered by the Disclosing Party to be confidential;
 - (ii) is by its nature confidential or the Receiving Party knows or ought to know is confidential; or
 - (iii) is personal information for the purposes of the *Privacy Act 1988* (Cth) or the *Privacy and Personal Information Protection Act 1998* (NSW) or is health information for the purposes of the *Health Records and Information Privacy Act* (NSW) 2002.
- (b) relates to any person and has been provided to or is held by the Disclosing Party on a confidential basis.

Confidential Information may be acquired before, on or after the Commencement Date. Confidential Information includes the existence of this agreement and information about the students of the University.

Details means the details set out on the cover pages of this agreement.

Disclosing Party means the party who is disclosing information, including Confidential Information.

Excluded Information means information that the Receiving Party can establish is in the public domain other than through a breach of this agreement.

Receiving Party means the party who is receiving information, including Confidential Information.

1.2 Rules for interpreting this agreement

Headings are for convenience only and do not affect interpretation. The following rules also apply in interpreting this agreement.

- (a) A reference to:
 - (i) a legislative provision or legislation (including subordinate legislation) is to that provision or legislation as amended, re-enacted or replaced;
 - (ii) a document or agreement (including this agreement), or a provision of a document or agreement (including this agreement), is to that document, agreement or provision as amended, supplemented or replaced;
 - (iii) a party to this agreement or to any other agreement or document includes a successor in title, permitted substitute or a permitted assign of that party;
 - (iv) a person includes any type of entity or body of persons, whether or not it is incorporated or has a separate legal identity, and any executor, administrator or successor in law of the person; and
 - (v) anything (including a right, obligation or concept) includes each part of it.
- (b) A singular word includes the plural, and vice versa.
- (c) A word which suggests one gender includes the other genders.
- (d) If a word or phrase is defined, any other grammatical form of that word or phrase has a corresponding meaning.

2. Disclosure of Confidential Information

- (a) The Disclosing Party agrees to disclose to the Receiving Party during the Term certain Confidential Information solely for the Purpose and subject to the terms of this agreement.
- (b) Neither party is obliged to disclose any particular information to the other party.



- (c) The Receiving Party acknowledges that neither the Disclosing Party nor its representative makes any representation or warranty (express or implied) as to the accuracy, content, legality or completeness of the Confidential Information or is under any obligation to notify the Receiving Party if it becomes aware of any inaccuracy, incompleteness or change in the Confidential Information.

3. Confidential Information

3.1. Obligations of confidentiality

In consideration of the disclosure referred to in clause 2 the Receiving Party agrees, except as permitted by clause 3.3, to:

- (a) keep all Confidential Information confidential;
- (b) not disclose Confidential Information directly or indirectly in any form to anyone else;
- (c) not use or make a copy of any Confidential Information other than for the Purpose; and
- (d) not manufacture any product or use any process based on the Confidential Information or otherwise commercialise anything based on the Confidential Information.

3.2. Ownership of Confidential Information

The Receiving Party acknowledges that all Confidential Information which has or may come into the possession of the Receiving Party and all rights relating to that Confidential Information remain the property of the Disclosing Party.

3.3. Exceptions to obligations of confidentiality

The obligations in clause 3.1 do not apply to the Receiving Party if:

- (a) the Disclosing Party has first agreed in writing to the particular disclosure, use, or copying;
- (b) the information is disclosed to an officer or employee of the Receiving Party who needs to know the information concerned to perform its duties in relation to the Purpose; or
- (c) disclosure of any Confidential Information is required to comply with any applicable law or requirement of any government agency or regulatory body and the Receiving Party first informs the Disclosing Party of the intended disclosure and cooperates with the Disclosing Party to limit that disclosure as reasonably requested.

3.4. Security of Confidential Information

The Receiving Party must:

- (a) keep effective control of Confidential Information;
- (b) ensure that Confidential Information is secure from theft, loss, damage or unauthorised access or alteration;
- (c) ensure that its officers or employees do not disclose, use or copy Confidential Information except as permitted by this clause 3;
- (d) if required by the Disclosing Party obtain from each of its officers and employees to whom Confidential Information is disclosed, a written undertaking to comply with the obligations of the Receiving Party under this clause 3 in a form approved by the Disclosing Party;
- (e) notify the Disclosing Party of any suspected or actual unauthorised use, copying or disclosure of Confidential Information; and
- (f) provide assistance reasonably requested by the Disclosing Party in relation to proceedings the Disclosing Party takes, or threatens to take, against any person for unauthorised use, copying or disclosure of Confidential Information.

3.5. Return of Confidential Information

- (a) Subject to clause 3.6, at the conclusion of the Purpose or at the written request of the Disclosing Party, the Receiving Party must (at its expense) promptly:
 - (i) deliver to the Disclosing Party (or if in electronic form, erase or destroy and deliver evidence of erasure or destruction) all documents and other materials containing, recording or referring to Confidential Information which are in its possession, power or control; and
 - (ii) ensure that any person who receives the Confidential Information by the Receiving Party's authority returns the Confidential Information to the Disclosing Party in any form in which it is held (or if it is in electronic form, erases or destroys it and gives evidence of its erasure or destruction to the Disclosing Party).



- (b) The return or destruction of documents or materials does not release the Recipient from its obligations under this agreement.

3.6. Exceptions to return and destruction

- (a) The Receiving Party is not required to delete or destroy any electronic back-up media that have been created solely by their automatic or routine archiving or back-up procedures to the extent that the media are not easily segregated, are maintained in confidence and are not accessible to users of the electronic system.
- (b) The Receiving Party may retain a copy of a document or material containing Confidential Information:
- (i) if the Receiving Party is required to retain the document or material by law or for the internal auditing or reporting obligations of the Receiving Party; or
 - (ii) if the document or material forms part of any advice, opinion or due diligence report prepared by advisers of the Receiving Party in relation to the Purpose.

3.7. Privacy

The parties and their employees and agents must comply with both parties' obligations under the *Privacy Act 1988* (Cth), the *Privacy and Personal Information Protection Act* (NSW) and the *Health Records and Information Privacy Act* (NSW) 2002 in relation to Confidential Information.

3.8. Survival of obligations

The obligations in this clause 3 concerning Confidential Information survive the expiry of the Term.

4. General

4.1 Governing law

This agreement is governed by the laws of New South Wales and any dispute relating to it must only be referred to the courts of New South Wales and the federal courts of Australia.

4.2 Assignment

Neither party may assign its rights or obligations under this agreement without the prior written consent of the other party.

4.3 Giving effect to this agreement

Each party must do anything (including execute any document), and must ensure that its employees and agents do anything (including execute any document), that the other party may reasonably require to give full effect to this agreement.

4.4 Exercise of rights

The exercise of a right does not prevent any further exercise of that right or the exercise of any other right. Neither the exercise of a right nor a delay in the exercise of a right operates as an election or a variation of the terms of this agreement.

4.5 Operation of this agreement

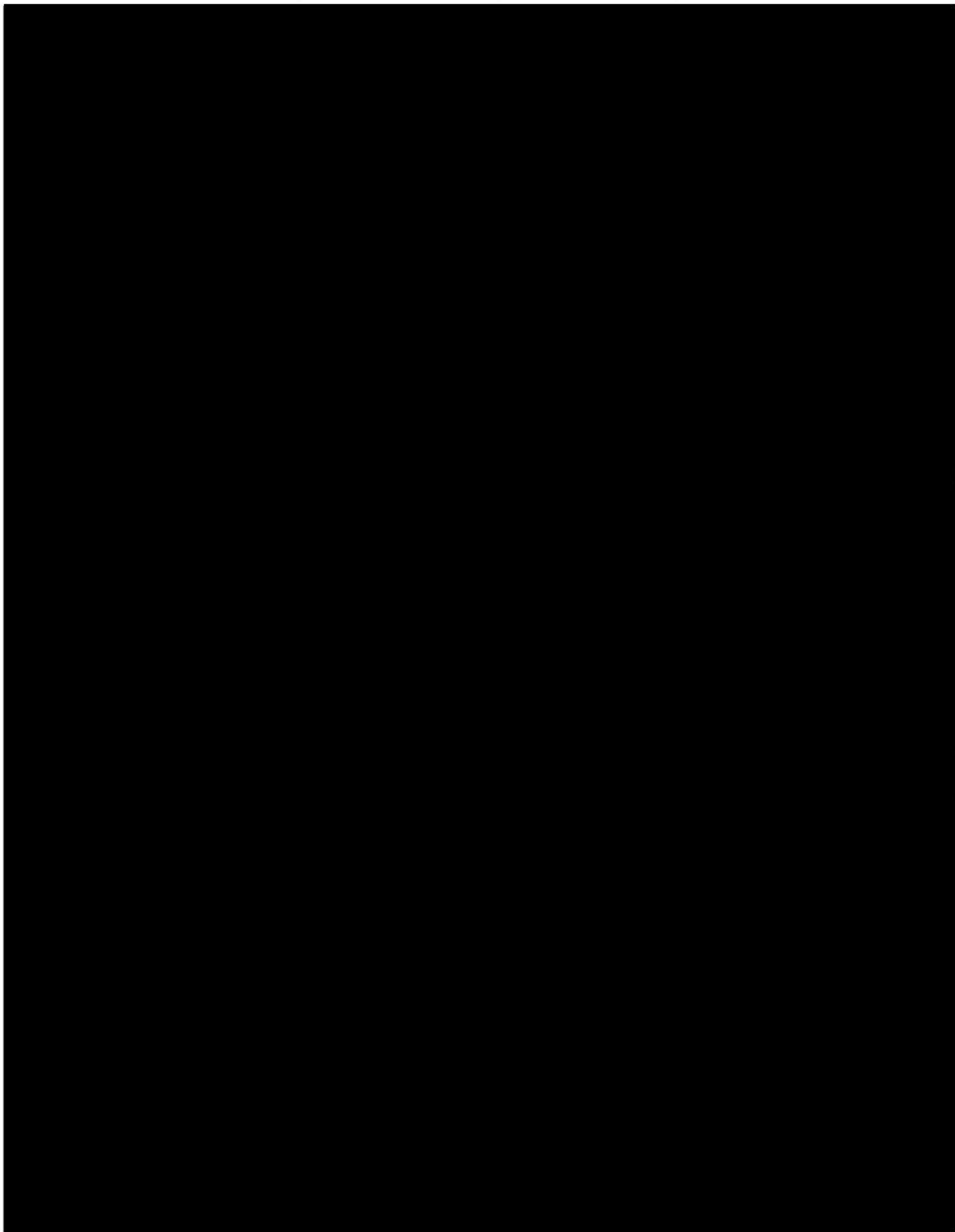
- (a) This agreement contains the entire agreement between the parties about its subject matter.
- (b) Any right that a person may have under this agreement is in addition to, and does not replace or limit, any other right that the person may have.
- (c) Any provision of this agreement which is unenforceable or partly unenforceable is, where possible, to be severed to the extent necessary to make this agreement enforceable.

4.6 Amendment

This agreement can only be amended by written agreement of the parties.

4.7 Counterparts

This agreement may be executed in counterparts.



Attachment 4

University Policies and Procedures

Computer and Network Security Procedure

Section 1 - Purpose

(1) This Procedure specifies the standards for cyber security protection for the University's computer and network resources in accordance with the [Cyber Security Policy](#).

Scope

(2) This Procedure applies to:

- a. all computer and network resources operated by, or on behalf of, the University (including its controlled entities); and
- b. all individuals, including third parties, involved in deploying and supporting computer and network resources for use by the University.

Section 2 - Policy

(3) Refer to [Cyber Security Policy](#).

Section 3 - Procedures

RESPONSIBILITIES AND REQUIRED ACTIONS

(4) It is the responsibility of all Macquarie Information Technology (IT) staff to understand the requirements of the University's Information Security Management System (ISMS) documented in this Procedure, specifically requirements relating to:

- a. Access Control;
- b. Building Secure Systems;
- c. Secure Development;
- d. Vulnerability Management;
- e. Vulnerability Risk Assessment;
- f. Network Security;
- g. Encryption;
- h. Logging and Monitoring; and
- i. Decommission and Destruction.

Part A - Access Control

(5) The University's IT resources must be configured to only permit authorised access to system functions and information.

Accounts

(6) The University will employ processes and systems to ensure the correct provisioning, review and removal of system and application accounts. A secure account management processes must be documented and followed to ensure:

- a. all individuals requiring access are provided with unique accounts that are named so that the account owner can be identified;
- b. approvals from an authorised staff member are obtained and recorded for each account requested;
- c. University staff are only provided with the access required to perform their job responsibilities;
- d. account privileges are restricted or removed if a staff member changes job roles in alignment with their new job responsibilities;
- e. access to the University email system is removed for accounts of academic staff three months after they leave the University's employment;
- f. access is removed for accounts for all other systems on the day they leave the University's employment;
- g. accounts are periodically reviewed to ensure access that is no longer required is revoked;
- h. accounts are disabled if unused for 180 days; and
- i. security events generated by user activity are logged to a central log repository.

Passwords

(7) The University's systems must enforce the following password restrictions. Passwords must:

- a. be at least eight characters in length;
- b. contain three of the character types: uppercase letters, lowercase letters, numbers, or special characters;
- c. not be the same as the previous five passwords chosen for that account;
- d. not be able to be changed more than once a day;
- e. be protected by a one-way hashing algorithm when stored; and
- f. not be displayed when they are entered during the login process.

(8) Systems must also employ measures to ensure that passwords are not guessable through the login interface. System must ensure that:

- a. accounts are locked out for 30 minutes after 15 consecutive failed login attempts.

(9) Access to applications that contain confidential, or highly sensitive information require multi-factor authentication, when accessed from off-campus locations.

Access Warning

(10) A message that discourages unauthorised access and notifies the user of activity monitoring must be displayed before a user attempts to logon to a system or application.

(11) For computer systems console access and network devices:

WARNING! This system belongs to Macquarie University. AUTHORISED ACCESS ONLY.

Access to this system is restricted to authorised users only. Actions performed by users on this system are logged and monitored. Activities conducted on this system that contravene the University's policies and procedures will be reported to the relevant authorities.

(12) For internal applications:

This application is operated by Macquarie University. Access to this application is restricted to authorised users only. Actions performed by users within this application are logged and monitored. Misuse of this application and its facilities will be reported to the relevant authorities.

Central Authentication

(13) Where technically possible, all systems and applications must authenticate users to a central authentication provider. The following controls must be in place:

- a. Use strong encryption for the transmission of username and password during the authentication process (e.g. Kerberos or LDAP over SSL) in accordance with the encryption requirements under the Encryption section of this Procedure.
- b. Pass-through authentication (single sign-on) is permitted unless the application facilitates access to "Highly Sensitive" information.
- c. User sessions must expire after 20 minutes of inactivity if facilitating access to "Highly Sensitive" information.

Database ACCESS

(14) Databases typically store large quantities of data. Access to databases containing production information must be strictly controlled:

- a. Non-production applications and databases must not contain production data.
- b. The System Administrator (SA) account must only be used in the case of an emergency; all direct access to databases must be conducted with the users unique ID.
- c. Applications that integrate with a database must be provided with a unique application account that is only used for interaction with the database by the application.
- d. Applications that allow users to access data directly from a database must log the identity of the user within user activity logs for data create, read, update, or delete activities.

Privileged Accounts and Passwords

(15) Administrator and super user accounts that have access to large quantities of information or privileged system functions, represent a significant risk to the University. Accounts that provide privileged access are subject to the following additional security requirements:

- a. must be approved by an authorised University officer or employee;
- b. must be assigned to an individual and be named so that the account owner can be identified;
- c. must enforce system access based on the role assigned to the individual;
- d. initial system access must be restricted to normal user access with a requirement to escalate privileges for privileged information access or functions; and
- e. must utilise multi-factor authentication.

(16) Privileged generic accounts, such as root, Administrator or enable, exist on almost all computers and network devices. Passwords for such accounts must:

- a. only be used in the case of an emergency;
- b. be reset to a randomly generated password of at least 16 characters at build time and at any time the password is communicated between staff members or third parties in the case of an emergency;

- c. be stored in a secure digital format protected by strong encryption;
- d. only be accessible by the minimum number of support staff required;
- e. not be communicated in the same communication medium as the system name and account name; and
- f. not be sent by email or computer based instant message technology. SMS, iMessage, or verbally over the phone is permitted.

Temporary Passwords

(17) Temporary passwords are required for the initial set-up of user accounts and the resetting of passwords for existing accounts. Temporary passwords can be sent via email but must:

- a. conform to the same complexity and length requirements as described under the Passwords section of this procedure;
- b. be unique to each occurrence of a new account or password reset request;
- c. require the user to change the password on next login; and
- d. expire after 24 hours.

Console Access

(18) Access to a system console constitutes access to the operating system's command line interface or graphical user interface. System consoles typically allow access to privileged functions and other applications and systems that the user is connected to. Console access must:

- a. require re-authentication after 20 minutes of inactivity; and
- b. not be directly accessible from the internet with a single factor of authentication.

System-to-System Accounts

(19) Connections between systems typically constitute privileged access for data transfer or automated system interactions. Credentials for system-to-system connectivity should have minimised handling only to initiate the connection between systems. System-to-system accounts must adhere to the following requirements:

- a. must not be used by individuals for day-to-day operations;
- b. must be either certificate based or consist of a password of at least 16 characters;
- c. must contain three of the character types: uppercase letters, lowercase letters, numbers, or special characters;
- d. can be set to never expire; and
- e. must be protected by strong encryption or restrictive file system permissions when stored (only permit access to the required application accounts).

Service and Application Accounts

(20) Service accounts are used by application and system services to perform automated operations. Service accounts can represent a risk to the University if not configured correctly. Service accounts must:

- a. be configured not to permit remote or direct console login;
- b. not be a root or administrator account for the underlying operating system;
- c. only be provided with the permissions required to perform its operations;
- d. have unique passwords (no identical passwords for service accounts across multiple systems);
- e. be named after the service or application that utilises the account;
- f. only be used for the purposes related to running or configuration of the relevant service or application; and

- g. be set with a randomly generated password of at least 16 characters (default passwords must be reset).

Access Via Mobile Devices

(21) Tablets and smartphones are typically not bound to a physical location and are exposed to meetings and locations with third parties and members of the public. Personal and University supplied mobile devices used to access the University's systems or information must:

- a. be protected by a PIN or password at least four characters long;
- b. require re-authentication after five minutes of inactivity; and
- c. have the ability to be remotely wiped.

Part B - Building Secure Systems

Secure Build and Configuration

(22) All computer systems built and configured for the purposes of University use, are subject to the following requirements:

- a. must be assigned a system owner and be registered in an asset database with system owner's name, business owner's name, computer name, IP address, and business purpose;
- b. must be located in an appropriate network zone in accordance with the Network Security section of this Procedure; and
- c. must be built in accordance with an applicable security baseline that includes the following configuration items:
 - i. The system clock must be synchronised with a trusted time provider.
 - ii. Must have unneeded services and software packages disabled or removed.
 - iii. Must have unneeded accounts removed, default credentials changed, and anonymous access disabled.
 - iv. Must be configured to deny network, shell, console, and file system access unless specifically permitted.
 - v. When commissioned into production, must have the relevant security patches applied that address security vulnerabilities for the deployed version.
 - vi. Must have media and network drive auto-play functions disabled.
 - vii. Must restrict privileged actions as well as access to configuration, log, and system files to administrator accounts only.
 - viii. Must log security events and privileged actions to a central log server in accordance with the logging requirements under the Logging and Monitoring section of this Procedure.
 - ix. Must be configured with a personal firewall if operating on premises that are not owned or operated by the University.
 - x. Must enforce secure user access in accordance with the Access Control section of this Procedure.

Protection from Viruses and Malware

(23) If the system runs a Microsoft Windows-based operating system, performs file transfer services, or is a public-facing web server, the system must:

- a. have centrally managed, real-time antivirus software installed;
- b. initiate an antivirus signature update at least every four hours; and
- c. have locally mounted disks scanned by antivirus software on a weekly basis.

Computer Systems That Handle Highly Sensitive Information

(24) To comply with regulations and industry standards, computer systems that handle Highly Sensitive information are required to comply with the following additional security requirements:

- a. Application whitelisting must be used to restrict application and script execution to only those folders or directories required to perform the business function.
- b. If not located in a locked cabinet within a datacentre, must have USB ports, floppy disk drives, and optical drives disabled.
- c. Must be monitored by change detection software that monitors critical system files and logs exception events to a central log server in accordance with the logging and monitoring requirements under the Logging and Monitoring section of this Procedure.
- d. Must log all data-level access to "Highly Sensitive" information to a central log server.

(25) The [Information Classification and Handling Procedure](#) provides further information about staff and student responsibilities for handling Highly Sensitive Information.

Part C - Secure Development

Security testing in the Software Development Life Cycle

(26) Following a documented and mature software development life cycle allows developers to incorporate tests for security issues early in the development process. Software written for use by the University should follow a standardised development life cycle that incorporates at least two security tests. For example, tests may take the form of a manual code review, static analysis or penetration test.

Web Application Development

(27) Web applications are commonly exposed to a large number of untrusted users. Developers must take additional precautions when developing web applications, including:

- a. implement protection from the OWASP Top 10 Web Application Security Risks.;
- b. scan for, and address vulnerabilities in accordance with the vulnerability management requirements under the Vulnerability Management section of this Procedure, after every change to the code or configuration of production software;
- c. if externally accessible, segment the web application into presentation, application, and database zones in accordance with network security requirements under the Network Security section of this Procedure; and
- d. restrict exposure to non-production applications to internal networks only.

Part D - Vulnerability Management

Vendor Security Advisories

(28) Software vendors regularly publish advisories notifying customers of their software that security vulnerabilities have been identified. Staff responsible for maintaining systems or applications must subscribe to the relevant advisories. This includes the following responsibilities:

- a. Staff responsible for supporting computer system infrastructure (desktops and servers) must subscribe to vulnerability advisories for operating systems and virtual server platforms in use by the University.
- b. Staff responsible for supporting network infrastructure must subscribe to vulnerability advisories for network devices and network management systems in use by the University.

- c. Staff responsible for supporting applications and databases must subscribe to vulnerability advisories for applications and database infrastructure in use by the University.
- d. Staff responsible for supporting security infrastructure (e.g. firewalls, antivirus, antispam, encryption, and VPN systems) must subscribe to vulnerability advisories for security infrastructure in use by the University.
- e. Security operations staff must subscribe to general security advisories from local and international authorities (e.g. AusCERT, US CERT, Stay Smart Online).

(29) Security vulnerabilities for software and systems in use by the University must be assessed for criticality. Alerts rated as high or critical must be actioned in accordance with the Vulnerability Risk Assessment section of this Procedure to ensure that University systems are patched as needed.

Part E - Vulnerability Risk Assessment

(30) A risk assessment must be conducted on vulnerabilities as they are published or advised by software and infrastructure vendors.

(31) The risk rating of a particular vulnerability is calculated by assessing the risk factors in Table 1: Risk Factors.

Table 1: Risk Factors

Risk factor	Risk rating = 1	Risk rating = 2	Risk rating = 5
Exposure	Local subnet	Campus network	Public access
Asset at risk	Public	Controlled	Confidential
Exploitation	Non-trivial	Not-public	Demonstrable
Execution	User interaction	Authenticated	Unauthenticated
Scope	1-5 systems	6-10 systems	> 10 systems

(32) The following Risk Rating calculation is then used to determine the risk that a vulnerability poses to the University:

$$\text{Risk rating} = \text{Exposure factor} + \text{Asset at risk factor} + \text{Exploitation factor} + \text{Execution factor} + \text{Scope factor}$$

Table 2: Risk Rating - severity and notification and response requirements

Risk Rating	Severity	Description	Notification	Response
> 17	Critical	The exploitation of the vulnerability presents an imminent threat with the potential of: 1. Exposing confidential information to unauthorised parties 2. Disrupting the operation of critical systems 3. Damage to the University's reputation	CIDO	Resolved in 48 hours
10 - 16	High	The exploitation of the vulnerability presents a likely threat with the potential of: 1. Exposing bulk controlled information to unauthorised parties 2. Disrupting the operation of important systems	IT Directors and Information Security Manager	Resolved within one month

Risk Rating	Severity	Description	Notification	Response
1 - 16	Medium - Low	The exploitation of the vulnerability presents a likely threat with the potential of: 1. Exposing a small amount of controlled information to unauthorised parties 2. Disrupting the operation of systems with limited users	System Owner and Information Security Manager	Resolved during normal patching cycle

Software Patching Cycles

(33) Software in use on University desktops, servers and network devices must reviewed for security patching on a regular basis. The frequency of review is based on the following exposure levels:

- a. Externally exposed (allows direct interaction from internet) – monthly review;
- b. Authenticated or internal access only – quarterly review.

(34) Timeframes for patching depend on the severity of the vulnerability determined by the risk assessment framework defined in the Vulnerability Risk Assessment section of this Procedure.

Part F - Network Security

Secure Network Environments

(35) All network environments owned, maintained, or operated by the University are subject to the following requirements:

- a. "Confidential" data, "Highly Sensitive" data and authentication credentials must be protected in transit by strong encryption in accordance with encryption requirements under the Encryption section of this Procedure.
- b. Firewalls must only allow the ports required for the business function and deny all other traffic.
- c. All network zones must be protected from the internet and third-party environments by a dedicated firewall system.
- d. Computer systems that require direct connection to external locations (inbound and outbound) must be located in a DMZ..
- e. All inbound traffic from external locations to internal systems (non-DMZ) must pass through a proxy or bastion host located in a DMZ that performs protocol inspection or conversion.
- f. Internet access provided by the University must be filtered to prohibit access to malicious or potentially dangerous sites.
- g. The firewall system protecting a computer system in the DMZ must not be configurable from the computer system it is protecting.
- h. Non-production environments must be separated from production environments by a dedicated firewall system.
- i. Key chokepoints between network zones must be monitored by intrusion detection and prevention systems that notify the Macquarie IT Cyber Security when an attack or violation of policy is detected.
- j. Console access to systems must not be directly accessible from the internet with a single factor of authentication.

Web Application Environments

(36) Network environments that host internet facing web applications are particularly susceptible to attacks from malicious parties. Special segmentation and traffic rules that protect web applications and limit exposure in the event of an attack are required. Web application environments must adhere to the following requirements.

© 2015 Macquarie University. All rights reserved. This document is the property of Macquarie University. It is to be used only for the purposes for which it is intended. It is not to be distributed, copied, reproduced, or otherwise used without the prior written permission of Macquarie University. For more information, please contact the Information Security team at 150 009 9734 or infosec@mq.edu.au.

- a. Must reside in at least a two-tier network architecture (application and database).
- b. Servers in the database zone must not be permitted to initiate connections directly with the application zone.
- c. Servers directly involved in hosting internet-facing web applications must have outbound traffic to the general internet blocked.

Remote Access for Privileged Users

(37) Remote access allows trusted personnel to access the University's resources from remote locations. Strong authentication is required to ensure that access is authorised and access beyond a business need or staff employment is revoked. It is required that:

- a. remote access is authenticated by multi-factor authentication;
- b. remote access is removed immediately when no longer required;
- c. remote access traffic must be protected by strong encryption; and
- d. if provided for a specific task, remote access should be limited to the time period allocated for the task.

Network Device Security

(38) Switches, routers, and firewalls facilitate the transmission of University information and access to all University applications. All network devices must be configured to protect against unauthorised access and malicious attack. Requirements are that:

- a. unneeded accounts are removed and default credentials changed;
- b. unneeded services and software packages are disabled or removed;
- c. the system clock is synchronised with a trusted internal time source;
- d. secure user access is ensured in accordance with access control requirements under the Access Control section of this Procedure;
- e. security events are logged to a central log server;
- f. when commissioned into production, must have the relevant security patches applied that address security vulnerabilities for the deployed software version;
- g. a patching cycle is maintained in accordance with the Vulnerability Management section of this Procedure; and
- h. the network device is located in a physically secure area that protects against tampering or theft.

Firewall and Network Change Approval

(39) Firewall rule changes must be reviewed and approved by Macquarie IT Cyber Security if they meet one or more of the following conditions:

- a. permit traffic to or from external (internet or third party) locations;
- b. permit traffic between production and non-production environments;
- c. permit a large number of source or destination addresses (greater than 10);
- d. permit all source or destination protocols (an "ANY" rule);
- e. permit a broad range of source or destination protocols (greater than a range of 20 ports);
- f. establish a new network path to an external party;
- g. use protocols that pass credentials or data in clear text (SNMP, POP3, IMAP, LDAP, FTP, TFTP, Telnet, rlogin, rsh);
- h. use protocols that are known as an avenue for computer worms (SMB/CIFS TCP445 & TCP139, MS-RPC TCP135, RDP TCP3389); and
- i. facilitate remote control of computers (RDP TCP3389, VNC TCP5500 TCP5800 TCP5900, pcANYWHERE TCP5631

Part G - Encryption

Approved Encryption Methods

(40) Protection of information with cryptography or hashing must employ the following algorithms and minimum key lengths.

(41) Symmetric encryption:

- a. Advanced Encryption Standard (AES) - 128-bit keys
- b. Triple Data Encryption Standard (DES) - 168-bit keys

(42) Asymmetric encryption:

- a. Rivest, Shamir and Adlemen (RSA) - 2048-bit keys

(43) Hashing:

- a. Secure Hashing Algorithm 2 (SHA-2) - 256-bit digest length

(44) Password encryption:

- a. Password-Based Key Derivation Function 2 (PBKDF2)
- b. Bcrypt
- c. Argon2

TLS Certificates, encryption and protocols

(45) Application access and data transfers that are secured by TLS (also known as SSL) must be conform to the criteria below:

- a. All versions of SSL (1, 2 & 3) must be disabled;
- b. The TLS version must be 1.2 or above;
- c. Certificates must be signed with SHA-256 certificates and certificate chains;
- d. Asymmetric key length must be 2048 or higher; and
- e. If Diffie-Hellman is used for key exchange, a 2048-bit group must be used.

(46) Additional validation is required for internet-facing websites:

- a. Certificates must be signed by a well-established commercial certificate authority; and
- b. Certificates must have, at most, a three-year validity period.

(47) For system-to-system interfaces:

- a. Certificates may be self-signed ;and
- b. Certificates may be valid for up to six-years.

Secure Encryption Key handling

(48) Keys used for encryption must be protected when transmitted or stored:

To help you find the correct answer, the correct answer is: (40) Protection of information with cryptography or hashing must employ the following algorithms and minimum key lengths. (41) Symmetric encryption: a. Advanced Encryption Standard (AES) - 128-bit keys b. Triple Data Encryption Standard (DES) - 168-bit keys (42) Asymmetric encryption: a. Rivest, Shamir and Adlemen (RSA) - 2048-bit keys (43) Hashing: a. Secure Hashing Algorithm 2 (SHA-2) - 256-bit digest length (44) Password encryption: a. Password-Based Key Derivation Function 2 (PBKDF2) b. Bcrypt c. Argon2 TLS Certificates, encryption and protocols (45) Application access and data transfers that are secured by TLS (also known as SSL) must be conform to the criteria below: a. All versions of SSL (1, 2 & 3) must be disabled; b. The TLS version must be 1.2 or above; c. Certificates must be signed with SHA-256 certificates and certificate chains; d. Asymmetric key length must be 2048 or higher; and e. If Diffie-Hellman is used for key exchange, a 2048-bit group must be used. (46) Additional validation is required for internet-facing websites: a. Certificates must be signed by a well-established commercial certificate authority; and b. Certificates must have, at most, a three-year validity period. (47) For system-to-system interfaces: a. Certificates may be self-signed ;and b. Certificates may be valid for up to six-years. Secure Encryption Key handling (48) Keys used for encryption must be protected when transmitted or stored:

- a. Keys must only be provided to those who have a business need to handle the keys.
- b. Keys must be protected by strong encryption during delivery to technical staff.
- c. Application keys or private keys for scripts, needed at system startup, must be stored in a location with read permissions only for the application or script user. All other permissions must be removed.
- d. Passwords used to encrypt keys must be at least 12 characters and must contain three of the character types: uppercase letters, lowercase letters, numbers, or special characters.
- e. Passwords to decrypt keys must not be sent by email or computer based instant message technology. SMS, iMessage, or verbally over the phone is permitted.
- f. Key encrypting keys must be stored separately to data encrypting keys.
- g. Keys must be stored in a single encrypted location that is regularly backed up to an encrypted repository.
- h. Keys must be replaced if they are no longer considered strong by industry standards or if there is a suspicion of exposure to unauthorised parties.

Part H - Logging and Monitoring

(49) The University will implement a practical and appropriate level of logging and monitoring to ensure that malicious events are identified and there is sufficient information to investigate and identify the origin of incidents.

Security events to be Logged

(50) Successful and unsuccessful attempts to initiate the following events must be logged:

- a. account log-on and log-off;
- b. password resets;
- c. account lockouts;
- d. user and group creation, modification, or removal;
- e. privilege escalation;
- f. actions taken by privileged users (root, sa, Administrator, enable);
- g. modification of system configuration;
- h. access to "Highly Sensitive" information (refer the [Information Classification and Handling Procedure](#) for a definition) ;
- i. modification of security logs;
- j. starting and stopping of system security services (e.g., logging, antivirus, file change detection, firewall);
- k. system or application errors and warnings; and
- l. activities invoked by scheduling systems.

Security event Log Contents

(51) Security logs must include enough information to identify the nature of the events as well as to attribute the event to an individual or system. To adequately identify the origin of events and provide insight into an incident, security logs must include:

- a. user account name;
- b. date and time stamp;
- c. origin of the event (IP address or DNS name);
- d. description of the event including the affected system object, file, or user;
- e. system in which the event occurred; and
- f. indication of activity success or failure.

Central Logging

(52) Where possible, applications and systems must send logs in real-time to the central security logging and monitoring system. Logs sent to the central system must:

- a. be retained for immediate access for one month; and
- b. be monitored for malicious events by an automated log correlation and alerting tool.

Part I - Decommission and Destruction

(53) University records must be retained in accordance with the [Records and Information Management Policy](#). Information that is not required to be retained for regulatory or University purposes on printed material or in a digital format must be securely destroyed so that the information is not able to be recovered by unauthorised parties. Destruction of University records must be approved by an authorised staff member and documented as a record itself.

System Decommission

(54) Systems that are decommissioned must have their network and IT support references removed. This includes removing:

- a. associated firewall rules and IP access control lists;
- b. VPN profile associations;
- c. forward and reverse DNS entries;
- d. entries in support databases such as the CMDB;
- e. system specific domain-level service accounts; and
- f. deletion of virtual machines and associated virtual disks.

Destruction of Printed Material

(55) Printed documents must be destroyed by using secure facilities provided by the University:

- a. by depositing in a locked secure destruction bins supplied by a AAA certified National Association for Information Destruction organisation; or
- b. By use of a DIN 66399 security level P-4 to DIN 66399 security level P-7 document shredder.

Destruction of Optical Media

(56) Optical media can contain significant amounts of information and must be destroyed when no longer needed. The following are acceptable methods of destroying optical disks:

- a. by safely cutting into four similar sized pieces with a pair of scissors;
- b. by use of a DIN 66399 security level P-4 to DIN 66399 security level P-7 document shredder that has CD and DVD shredding capabilities; or
- c. by disposal through a AAA certified National Association for Information Destruction organisation (a certificate of destruction must be obtained).

Repurposing Equipment

(57) Systems that are being repurposed must have their storage devices wiped before being deployed into their new function. The wiping procedure must adhere to the following:

- a. include at least a three-pass zeroing of all addressable locations; and

- b. a screenshot must be captured of the successful wipe operation and provided to Macquarie IT Cyber Security.

Equipment Disposal by a Third Party

(58) Systems that are being decommissioned and passed on to a third party for disposal must have their storage devices securely wiped either before providing to the third party or by the third party with adequate proof of destruction. If the third party is performing the data destruction the following requirements must be met:

- a. The third party must be AAA certified with the National Association for Information Destruction.
- b. The third party must provide a certificate of destruction for each storage device provided.
- c. The serial number of each device must be catalogued before destruction and listed in the certificate of destruction.

Wiping of Network Devices

(59) Network devices contain information relating to the University's internet network environment and communications links. In some cases, network devices contain VPN passwords, encryption keys, and network configuration details. Information contained on network devices must be securely wiped if being decommissioned, disposed of, or repurposed.

- a. Network device configuration must be reset to the factory default in accordance with the manufacturer's instructions
- b. Hard disks contained within network devices must be destroyed in accordance with the Decommission and Destruction section of this Procedure or securely wiped.

Section 4 - Guidelines

(60) Nil.

Section 5 - Definitions

(61) Commonly defined terms are located in the University [Glossary](#). The following definitions apply for the purpose of this Procedure:

- a. DMZ is a short name for a "demilitarised zone". A DMZ consists of a network zone within the University network that sits between an external and untrusted network zone and an internal protected network zone. DMZ networks typically hold externally accessible systems that are screened or filtered from access to internal systems.
- b. Malicious or dangerous sites are external network locations that are known to host malware or deceptive content such as fake websites used for phishing. These sites may be able to infect a computer with viruses or steal the usernames and passwords.

Status and Details

Status	Current
Effective Date	29th April 2021
Review Date	29th April 2024
Approval Authority	Vice-President, People and Services
Approval Date	29th April 2021
Expiry Date	Not Applicable
Responsible Executive	Nicole Gower Vice-President, Professional Services
Responsible Officer	[REDACTED] Chief Information and Digital Officer +61 2 9850 1660
Enquiries Contact	[REDACTED] Chief Information Security Officer +61 2 9850 1987 Information Technology

Modern Slavery Policy

Section 1 - Purpose

(1) This Policy sets out the University's commitment to:

- a. identify, assess, and minimise the risks of modern slavery in its operations and supply chains; and
- b. maintain responsible and transparent operations and supply chains.

(2) The University opposes all forms of modern slavery and is committed to respecting and protecting the human rights of the University community.

Background

(3) The term 'modern slavery' describes situations where coercion, threats or deception are used to exploit people and undermine or deprive them of their freedom. It broadly includes serious exploitative practices including human trafficking, slavery, forced labour, child labour, and other slavery-like practices.

(4) The University complies with the [Modern Slavery Act 2018](#), which requires the University to report annually on the steps which it takes to assess and address the risks of modern slavery in its operations and supply chains.

(5) The University expects its staff, affiliates, and controlled entities to work together to give effect to the principles set out in this Policy.

Scope

(6) This Policy applies to all University:

- a. staff;
- b. affiliates; and
- c. controlled entities.

Section 2 - Policy

University commitment

(7) The University is committed to ensuring that:

- a. University operations and supply chains do not cause, involve, or contribute to modern slavery;
- b. University contractors, suppliers, collaborators, and others with whom the University does business respect and share the University's commitment to minimising modern slavery risk; and
- c. the effectiveness of measures to ensure continual process improvement is evaluated.

External engagement

(8) All individuals engaging on behalf of the University (and its controlled entities) with external contractors, suppliers, collaborators, and others are required to:

- a. undertake risk-based assessments and due diligence, to minimise the risk of modern slavery in the University's supply chain;
- b. where appropriate and as informed by their risk assessment, engage with their contractors, suppliers, collaborators, and others to gain a proper understanding of the measures they have in place to identify and address modern slavery risks, including if applicable by requiring compliance with the University's [Supplier Code of Conduct](#).

Awareness

(9) The University will promote awareness of modern slavery through training and the availability of materials and practical tools to University staff, affiliates, and controlled entities to identify and address modern slavery risks.

Reporting

(10) The University encourages staff, affiliates, and others to raise concerns about potential modern slavery in the University's operations and/or supply chains through the [Complaint Management Procedure for Staff](#) or the [Complaints Resolution Policy for Students and Members of the Public](#).

Section 3 - Procedures

(11) Nil.

Section 4 - Guidelines

(12) Nil.

Section 5 - Definitions

(13) Commonly defined terms are located in the University [Glossary](#). The following definitions apply for the purpose of this Policy:

- a. affiliate means persons holding Honorary titles with the University, consultants and contractors, and volunteers working for the University;
- b. modern slavery has the same meaning as the [Modern Slavery Act 2018](#); and
- c. staff means all persons employed by the University, including continuing, fixed-term, and casual staff members.

Status and Details

Status	Current
Effective Date	24th May 2022
Review Date	24th May 2025
Approval Authority	Vice-President, Finance and Resources
Approval Date	24th May 2022
Expiry Date	Not Applicable
Responsible Executive	Robin Payne Vice-President, Finance and Resources
Responsible Officer	Robin Payne Vice-President, Finance and Resources
Enquiries Contact	Natalie Budovsky Chief Procurement Officer +61 2 0418 487 286

Health and Safety Policy

Section 1 - Purpose

(1) This Policy establishes the University's commitment to the principles and practices of workplace health and safety (WHS) in order to protect the health and safety of the University Community and environment.

Background

(2) The University is committed to providing a safe and healthy workplace that supports the proactive identification and management of safety risks in all activities of the Macquarie University Group. This commitment enables the University to achieve its strategic priorities detailed in [Our University: A Framing of Futures](#) and in alignment with relevant legal obligations.

Scope

(3) This Policy applies to all workers, students, and other persons associated with the University and controlled entities in the course of endorsed activities on and outside the University's campus. This is collectively identified as the Macquarie University Group. It is acknowledged that controlled entities may require additional policies and procedures for their own needs to reflect the culture, structure and purpose of their organisation. Any such documents will operate in alignment with this Policy.

Section 2 - Policy

(4) The University is committed to maintaining the health and safety of the University Community.

(5) To enable the Macquarie University Group to provide a healthy and safe workplace, the University will:

- a. ensure effective governance and oversight of the Macquarie University's Group's performance in health and safety;
- b. develop and enhance a proactive safety culture and necessary WHS capability;
- c. provide support and guidance through the implementation of a health and safety management system that complies with WHS legislation and adopts the principle of continuous improvement;
- d. establish and monitor measurable objectives for health and safety, targeting continual improvement for eliminating injury and illness;
- e. allocate suitable financial and physical resources to enable the University Community to perform safely and in accordance with legislation and the values of the Macquarie University Group;
- f. establish consultation and communication channels enabling the Macquarie University Group to discuss and resolve health and safety matters;
- g. provide safe and suitable equipment and infrastructure for Macquarie University Group activities; and
- h. implement a return to work program to support staff who have been harmed or injured to return to work in a safe and timely manner.

Roles and Responsibilities

University Officers

(6) The University Officers, as per the [Work Health and Safety Act 2011](#) (NSW), are responsible for:

- a. maintaining their knowledge of health and safety matters;
- b. ensuring there are appropriate resources and processes to eliminate or minimise health and safety risks;
- c. ensuring there are processes in place to receive information about incidents, hazards and risks in a timely manner;
- d. ensuring processes are in place to comply with a duty within the WHS legislation and associated regulations as they relate to the delivery of academic and professional endorsed activities; and
- e. verifying the provision and resources for the above.

Vice-Chancellor

(7) The Vice-Chancellor is responsible for overseeing the performance of the Macquarie University Group regarding WHS and undertaking activities to address due diligence obligations.

Faculty Executive Directors, Heads of Departments and Unit Managers

(8) Faculty Executive Directors, Heads of Departments, and managers within academic and professional units are responsible for the following within their area of management:

- a. promoting safety as central to the area's culture and a key consideration in daily operational activities;
- b. ensuring that the safety management system of the Macquarie University Group is actively implemented;
- c. ensuring that safety consultation arrangements are established and effective;
- d. ensuring appropriate resourcing for health and safety;
- e. ensuring that worker's and student's skills and knowledge are current and adequate given the specific safety risks and competency needs of their work area; and
- f. consulting with University Community members so that health and safety issues are raised, addressed, and resolved in a timely manner.

Supervisors

(9) Supervisors (including academic supervisors) within academic and professional units are responsible for the following within their area of management:

- a. promoting a safe workplace where health and safety matters are resolved in consultation with stakeholders;
- b. encouraging incident reporting, leading incident investigations and implementing control measures;
- c. ensuring that activities, operations, and equipment are safely managed using the University risk management process and that applicable safe working instructions and procedures for hazardous activities are in place;
- d. engaging in the injury management process when a University Community member sustains an injury;
- e. educating and informing the workplace through the distribution of information and training to ensure WHS competency; and
- f. monitoring the workplace to ensure hazards are controlled to eliminate and / or minimise health and safety risks.

Manager - Specialised Safety Risk or Infrastructure

(10) A manager of a specialised safety risk or infrastructure is responsible for:

- a. ensuring that operations and equipment are safely managed using University risk management processes;
- b. consulting with University Community members to raise and address health and safety issues;
- c. providing information and suitable training to University Community members about health and safety risks and control measures;
- d. contributing to ensure effective development and adoption of relevant policies and procedures in conjunction with the Workplace Health and Safety Unit; and
- e. participating and contributing to incident investigations and assisting with the implementation of corrective actions.

Workers and Students

(11) Workers and students are responsible for:

- a. taking reasonable care for their own health and safety and not adversely impacting the health and safety of others;
- b. following reasonable safety instructions and directions from University Managers or Supervisors; and
- c. reporting health and safety injuries, hazards, and near miss events via the Macquarie University's Group's [ROAR - Risk Online Active Reporting](#) system.

The Workplace Health and Safety Unit

(12) The Workplace Health and Safety Unit is responsible for:

- a. creating an informed and educated workplace by distributing technical advice regarding health and safety matters;
- b. ensuring strategic focus through the facilitation of health and safety goals determined by the University Council, University Executive Group, and academic and professional units;
- c. developing efficient processes and systems by facilitating training and tools which are embedded into the diverse operations of the Macquarie University Group; and
- d. addressing emerging and upcoming changes by disseminating up to date information regarding changes in health and safety laws, and the Health and Safety Management System.

Health and Safety Committees

(13) The Macquarie University's Group Health and Safety Committees are responsible for:

- a. discussing, setting, and monitoring health and safety goals;
- b. implementing health and safety initiatives to control health and safety risks within their area of control;
- c. resolving systemic health and safety issues within their area of control (note: individual injuries are not discussed by these committees); and
- d. providing feedback to managers of the relevant Faculty, Deputy Vice-Chancellor Office, or controlled entity on matters relating to health and safety processes and systems.

Health and Safety Representatives

(14) Health and Safety Representatives have the following functions within their Work Group:

- a. participating in effective communication strategies between workers in a Work Group and with management;
- b. investigating and consulting the University Community regarding complaints and issues raised in the Work Group; and
- c. initiating health and safety issue resolution procedures and escalating health and safety issues to managers of

the relevant Faculty, Deputy Vice-Chancellor Office, controlled entity or Health and Safety Committee. A Health and Safety Representative may engage Workplace Health and Safety for additional action or support where necessary.

Section 3 - Procedures

(15) Nil.

Section 4 - Guidelines

(16) Nil.

Section 5 - Definitions

(17) Commonly defined terms are located in the University [Glossary](#). The following definitions apply for the purpose of this Policy:

- a. Hazard means a source of potential harm or injury;
- b. Health and Safety Committees means Committees of the Macquarie University Group that represent and consult with members of the University Community. These committees identify health and safety related matters within their Work Group, devise initiatives, and implement solutions to improve the health and safety of their area;
- c. Health and Safety Management System means the comprehensive management system that includes organisational structure, planning activities, responsibilities, procedures, processes, tools and resources to manage health and safety risk for the Macquarie University Group;
- d. Health and Safety Representative means a worker elected by members of a Work Group to represent other workers in matters relating to health and safety;
- e. Manager - Specialised Safety Risk or Infrastructure means an employee in a managerial position who is responsible for a specialised health and safety risk (e.g laser, diving, fieldwork) or infrastructure such as a laboratory or other technical facility;
- f. Near Miss Event means a health and safety incident that occurred where a person could have been injured however, no injury was sustained;
- g. Officer: As defined in the [Work Health and Safety Act 2011](#) (NSW), the term Officer refers to a director or executive officer of the organisation; or a person who makes, or participates in making, decisions that affect the whole, or a substantial part of the organisation; or a person who has the capacity to significantly affect the organisation's financial standing.
- h. Other persons means conference or event attendees, patrons, patients, members of the public on campus, research participants, guests, delegates, and visiting colleagues from other organisations;
- i. Safety Risk means the possibility that harm (death, injury or illness) might occur when exposed to a hazard;
- j. Specialised Safety Risk means a safety risk that includes specialist or scientific principles, for example, but not limited to: chemical, laser, electrical, radiation, biological, diving, fieldwork, etc.;
- k. Student means a person enrolled in a program or unit of study provided by the University including a person in a pathway programme, an undergraduate or postgraduate program, a cotutelle program or a visiting student;
- l. Supervisor means a worker or student appointed in an academic or professional unit to oversee endorsed activities, work performance, and duties undertaken by workers and / or students to ensure they are performed according to the standards and values of the Macquarie University Group;
- m. University Community means workers, students, and other persons associated with Macquarie University Group

endorsed activities;

- n. Macquarie University Group or Group means Macquarie University and its Controlled Entities;
- o. Worker means a person associated with the Macquarie University Group as an employee, officer, trainee, volunteer, honorary fellow, appointee to conjoint, adjunct, emeritus, honorary, clinical and visiting academic position, contractor, sub-contractor, apprentice, or in work experience;
- p. Work Group means a group of University Community members that have similar hazards and safety risks within an academic or professional unit;
- q. Workplace means a place where work is carried out for the Macquarie University Group, including a place connected to the Macquarie University Group's endorsed activities where a worker goes or is likely to go.

Status and Details

Status	Current
Effective Date	21st February 2021
Review Date	18th February 2023
Approval Authority	Vice-President, People and Services
Approval Date	29th August 2018
Expiry Date	Not Applicable
Responsible Executive	Robin Payne Vice-President, Finance and Resources
Responsible Officer	Lance Islip Manager, Workplace Health and Safety +61 2 9850 9723
Enquiries Contact	Lance Islip Manager, Workplace Health and Safety +61 2 9850 9723

Acceptable Use of IT Resources Policy

Section 1 - Purpose

(1) This Policy specifies requirements for the respectful, safe, reliable and secure use of Information Technology (IT) Resources provided by the University.

Background

(2) Information Technology Resources are vital for delivering the University's activities. The University is committed to maintaining a respectful, safe, reliable, and secure technology environment that allows the University to meet its organisational objectives, legal requirements, and ethical responsibilities.

Scope

(3) This Policy applies to:

- a. all technology resources used by, operated by, or provided on behalf of the University (including its controlled entities);
- b. all information collected, created, stored, or processed by, or for, the University on computer and network resources; and
- c. all individuals who utilise, or are involved in deploying and supporting, computer and network resources provided by the University.

Section 2 - Policy

ACCEPTABLE USE

(4) All individuals who access, use or otherwise engage the University's IT Resources are required to:

- a. respect the rights of all individuals, including other users;
- b. only use or modify University IT Resources for Authorised Purposes, and not in breach of relevant laws or contractual obligations;
- c. not use University computer or network equipment for non-commercial personal purposes beyond a reasonable amount, or to the detriment of the University or its goals;
- d. not access, distribute, store or display illegal, pirated or offensive material;
- e. not use University computer or network equipment for unauthorised personal financial or commercial gain;
- f. not misrepresent the views of the University, via use of the University's IT Resources;
- g. not conduct activities that consume excessive network bandwidth;
- h. report suspected or actual security breaches to the Information Technology (IT) Service Desk in a timely manner; and
- i. maintain the security and confidentiality of information generated or collected by the University in accordance with the Information Classification and Handling Procedure.

SECURE SYSTEM ACCESS AND USE

(5) To protect access to University IT Resources, individuals are required to:

- a. select long and strong passwords that are not easily guessed and not in use in other non-University applications;
- b. not share University-provided or self-selected passwords with other individuals;
- c. keep personal and University-provided systems, used to access University systems or information, free from known vulnerabilities by keeping up-to-date with vendor provided security updates;
- d. maintain operational and up-to-date antivirus on personal and University-provided systems used to access University systems or information;
- e. securely store passwords that provide access to University systems or information;
- f. only use the accounts provided by the University for their own individual use;
- g. not bypass or attempt to circumvent the University's Security Controls or Protection Mechanisms;
- h. not introduce malicious software such as viruses, worms, ransomware or trojans into the University environment; and
- i. not use Hacking Tools (including sniffing, scanning, password guessing or exploitation) when accessing, using or otherwise engaging with University IT Resources.

MONITORING AND COMPLIANCE

(6) The University monitors its information systems for compliance with this Policy in accordance with the University's Workplace Surveillance Policy. Breaches of this Policy constitute misuse of University's information and information systems.

(7) The [Acceptable Use of IT Resources - Misuse Schedule](#) provides some examples of activities that constitute misuse of IT Resources. If misuse of IT Resources is detected or suspected, relevant disciplinary provisions will be invoked.

(8) The University may refer serious matters or repeated breaches to the Chief Information and Digital Officer, Chief People Officer, the Head of the relevant organisational unit, or the appropriate external authorities which may result in disciplinary and / or civil, and / or criminal proceedings.

(9) The University has a statutory obligation to report illegal activities and corrupt conduct to appropriate authorities and will cooperate fully with the relevant authorities.

(10) To the extent allowed by law, the University is not liable for loss, damage or consequential loss or damage arising directly or indirectly from the use or misuse of any Information Technology Resources.

Section 3 - Procedures

(11) Nil.

Section 4 - Guidelines

(12) Nil.

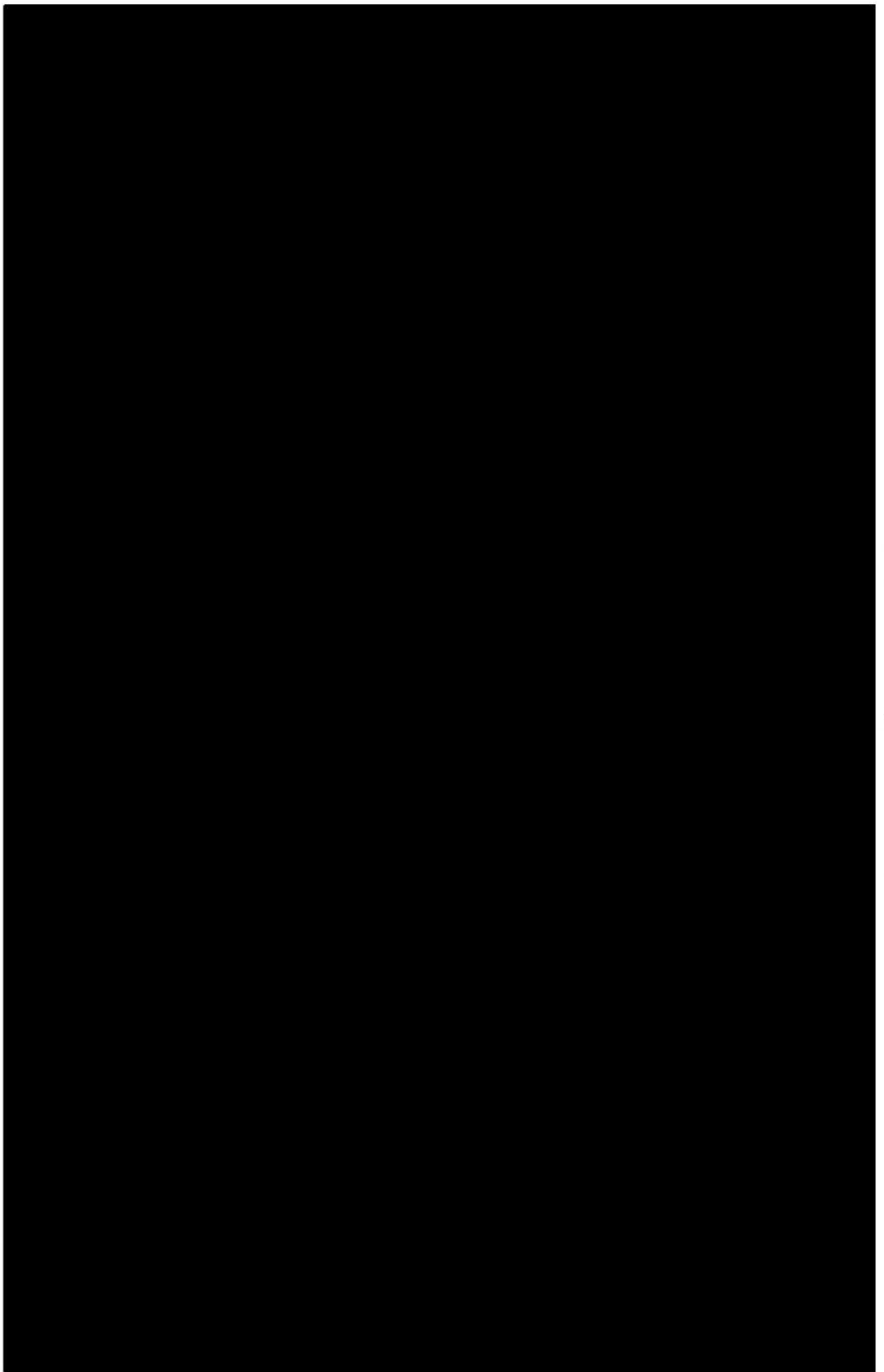
Section 5 - Definitions

(13) Commonly defined terms are located in the University [Glossary](#). The following definitions apply for the purpose of this Policy:

- a. **Authorised Purposes** means activities associated with work or study at the University, or provision of services to or by the University, which are approved or authorised by the relevant officer or employee of the University in accordance with University policies and procedures or pursuant to applicable contractual obligations, limited personal use, or any other purpose authorised by the relevant officer or employee.
- b. **Hacking Tools** means tools that are designed to facilitate the identification and exploitation of software or system weaknesses for the purposes of unauthorised access.
- c. **Information Technology Resources, or IT Resources**, includes, but is not limited to:
 - i. All computers and all associated data networks and systems, internet access and network bandwidth, email, hardware, data storage, computer accounts, all OneID systems, media, software (both proprietary and those developed by the University) and telephony services.
 - ii. Information Technology services provided jointly, or as part of a joint venture between the University and a research centre, school, institute affiliated with the University, a subsidiary organisation owned by the University or any other partner organisation.
 - iii. Information Technology services provided by third parties that have been engaged by the University.
- d. **Security Controls or Protection Mechanisms** means systems or facilities implemented to restrict access only to individuals who are authorised to access or utilise the resource or information.

Status and Details

Status	Current
Effective Date	28th April 2021
Review Date	28th April 2024
Approval Authority	Vice-President, People and Services
Approval Date	28th April 2021
Expiry Date	Not Applicable
Responsible Executive	Nicole Gower Vice-President, Professional Services
Responsible Officer	[REDACTED] Chief Information and Digital Officer +61 2 9850 1660
Enquiries Contact	[REDACTED] Chief Information Security Officer +61 2 9850 1987





MACQUARIE
University

Powered by
Adobe
Acrobat Sign