Health Systems Support Framework
NHS Digital Staff Passports Service
Order Form

Contract Title	C60678_NHS Digital Staff Passports Service
Order Reference Number	600208652
Date of Order Form	24th March 2022
Authority	NHS Commissioning Board (Known as NHS England)
Supplier	Sitekit Applications Ltd (Prime supplier)
Status of Order Form	Issue of this Order Form is an "invitation to treat" by the Authority following the Suppliers' Call-Off ITT Response submitted by the Supplier(s) in response to the relevant mini-competition conducted under and in accordance with the Framework Agreement. On the signature of the Order Form by the Suppliers and its return to the Authority, the signature of the Order Form by the Authority shall be the point at which a contract is formed between the Authority and the Suppliers. This Order Form, together with the Call-Off Terms and Conditions and the applicable provisions of the Framework Agreement (and the other provisions as set out in the Call-Off Terms and Conditions) form a contract (defined as "the Contract" in the Call-Off Terms and Conditions) between the parties as at and from the date of this Order Form. All terms defined in the Call-Off Terms and Conditions have the same meaning when utilised in this Order Form.
Call-Off Terms and Conditions	The Call-Off Terms and Conditions comprise the following Schedules of Appendix A of the Framework Agreement:

Schedule 1	Key Provisions
Schedule 2	General Terms and Conditions
Schedule 3	Definitions and Interpretations Provisions

	Schedule 4	This Order Form
	Schedule 5	Information Governance
	Schedule 6	Security Management
	Schedule 7	Standards
	Schedule 8	Software
	Schedule 9	Installation and Commissioning Services
	Schedule 10	Maintenance Services
	Schedule 11	Guarantee
	Schedule 12	Staff Transfer
	Schedule 13	Change Control Process
	Schedule 14	Calculation of Termination Sum
	Schedule 15	Standard Licence Terms
	Schedule 16	Acceptance Testing
	Any additional Extra Key Provisions set out at Annex 2 below shall be incorporated into the Contract formed by the signature and completion of this Order Form.	
Framework Agreement	The Health Systems Support Framework established by NHS England for and on behalf of NHS England and other contracting authorities and other organisations in relation to the provision of deliverables that may be required for the facilitation and support of sustainable transformation partnerships and/or integrated care systems (the "Framework Agreement") to which suppliers were appointed following their submission of responses to the framework ITT ("Framework ITT").	

Call-Off ITT	The Call-Off ITT as issued by the Authority to invite responses to the relevant mini-competition conducted under and in accordance with the Framework Agreement.
Call-Off ITT Response	The Suppliers' response to the relevant Call-Off ITT submitted by the Suppliers in response to the relevant mini-competition conducted under and in accordance with the Framework Agreement and initiated by the issue of a Call-Off ITT by the Authority.
Term of the Contract	11th April 2022 –17th January 2023
Extension of Term	On agreement by both parties in-line with the HSSF Terms and Conditions
Unilateral Authority right of termination notice period	6 months
Maximum Payments following Unilateral Authority right to terminate	N/A
Maximum Permitted Profit Margin	N/A – Capped Fixed Price Contract
Variation to Termination Sum calculation	N/A
Deliverables	The Deliverables to be provided by the Supplier(s) under the Contract shall be the Services and/or Ad Hoc Services and/or Goods and/or any other requirement whatsoever (including without limitation any item, feature, material, outcome or output) set out at Annex 1 to this Order Form ("the Specification") and shall be provided from the Deliverables Commencement Date set out below in accordance with the KPIs set out in the Specification. Where the Suppliers are comprised of more than a single Supplier the Supplier Matrix shall indicate which portion of the Deliverables are to be provided by which of the Suppliers. **Deliverables** 1. Supply of licenses for use of digital wallets and VC ecosystems, including trust list and status list. 2. Development and support for Wrapper SDK for interoperability with wallet stacks. Supply and

	maintenance of the code for the Condatis Credential Gateway. 3. During Alpha and Beta, Sitekit will provide Software as a Service Services on Standard Licence Terms as part of the Deliverables pursuant to this Contract, and in particular, will provide the Condatis Credential Gateway to the Authority in accordance with **Clause 16 of Schedule 2 of the Call-Off Terms and Conditions**, and the Authority shall not be entitled to use the source code and other deliverables of the NHS Community Edition, unless and until the licence set out under "Licensing of Intellectual Property" is granted. 4. Provide to the Authority the full source code, the design documents and technical information and a license (on the terms set out below under "Licensing of Intellectual Property") to use any proprietary tools and methodologies and all rights therein for the NHS Community Edition as available and up to date as at the date of delivery of the aforesaid. 5. Technical support service for selected digital wallet and VC ecosystems as defined by the SLA in Annex 1. 6. Administration of trust registers for the trusted frameworks, revocation lists and other similar trust registers. Specifically, to add or remove issuers and credential schema as notified by the NHS. The development and adoption of Trusted Frameworks in not in the scope of this Order Form. 7. Support the initial scope of permanent staff movements of Doctors in Training (DiT) employed by NHS organisations and for temporary staff movements for all staff employed by NHS organisations. The service will need to be scalable to cover all permanent and temporary staff movements between NHS organisations and extensible to enable staff movement into and out of the NHS.
Condatis Credential Gateway	As outlined in Annex [4].
NHS Community Edition	The specific NHS edition of Condatis Credential Gateway which is developed during Alpha.

Alpha	As outlined in Annex 3 and 4.
Beta	As outlined in Annex 3 and 4.
Priority Deliverable	As outlined in Annex 1
Deliverables Commencement Date	11th April 2022
Services Commencement Date	1st October 2022 (targeted)
Goods Commencement Date	N/A
Long Stop Date	31st March 2023
Implementation Plan	The implementation plan submitted as part of the Call-Off ITT Response and set out at Annex 4 below.
Information Security Management Plan	The information security management plan submitted as part of the Call-Off ITT Response (if required by the relevant mini-competition conducted in accordance with the Call-Off ITT) and set out at Annex 5 below, as may be amended from time to time in accordance with Schedule 6 of these Call-Off Terms and Conditions.
Insurance	As per the HSSF Call-Off Terms and Conditions.
Insurance on Expiry or Termination	On the expiry or earlier termination of this Contract, the Suppliers are required to ensure that: 1) unless otherwise required in the Extra Key Provisions, any ongoing liability that they have or may have arising out of this Contract shall continue to be the subject of appropriate insurance and/or indemnity arrangements and/or membership of the risk pooling statutory schemes for the period of six (6) years from termination or expiry of this Contract; and 2) where the Deliverables or any part of them could result in liability to any patient in respect of care and/or advice funded by an NHS body, any ongoing liability that the Suppliers have or may have arising out of this Contract

	shall continue to be the subject of appropriate insurance and/or indemnity arrangements and/or membership of the risk pooling statutory schemes for the period of up to twenty-one (21) years from termination or expiry of this Contract. (See Clauses 20.8 and 20.9 of Schedule 2 of the Call-Off Terms and Conditions, respectively)
Key Roles for the supply or performance of the Deliverables and the personnel who will fill those Key Roles ("Key Personnel")	Client Services / Account Manager – Michael Catania Programme / Project Manager – John Attwood Solutions Architect – Richard Astley Information Security Manager – John Yau Developer Lead – Donald Robertson QA / Testing Lead – Jamie Lennox Technical Services Manager – Jonathan Drever Customer Services Manager – Jasmine Taylor
Premises and Location(s) for the Delivery of the Deliverables	As this is a national programme of work, the supplier will need to be prepared to work with localities across England. In line with current operating models it is expected that most work will be undertaken remotely. Any travel arrangements should be made in line with government advice on Covid restrictions, with teams encouraged to work remotely as far as feasible.
Licence(s) and/or Lease(s) granted to the Suppliers	N/A
Information Governance Provisions (Schedule 5)	See Schedule 5 of the Call-Off Terms and Conditions.
Processing of Personal Data	See Schedule 5 of the Call-Off Terms and Conditions.
Intellectual Property	See Clause 14 of Schedule 2 of the Call-Off Terms and Conditions. The NHS Community Edition shall constitute Supplier Owned Foreground IPR for the purposes of this Order Form and the Call-Off Terms and Conditions. At the end of Alpha,

	Condatis will provide the Authority with the source code for the NHS Community Edition of the Condatis Credential Gateway (deliverable 3 of the Deliverables), on the terms of the licence below.
Licensing of Intellectual Property	During Alpha and Beta, the Prime Supplier will provide the Condatis Credential Gateway to the NHS Commissioning Board (Known as NHS England) on Software as a Service terms in accordance with Clause 16 of Schedule 2 of the Call-Off Terms and Conditions, and the NHS Commissioning Board (Known as NHS England) shall not be entitled to use the source code and other deliverables of the NHS Community Edition, unless and until the licence is granted below. In the event that the Contract is terminated for failure to deliver, or material breach, or expires, and is not replaced by any similar contract for Condatis Credential Gateway or any similar product, the NHS Commissioning Board (Known as NHS England) shall be entitled to use the NHS Community Edition on the following terms: • Non commercially exploitable • Non-transferable or sub-licensable • Non revokable • In perpetuity • Usable only by the Authority or successor organisations in England and only in the field of Health and Social Care. For the avoidance of doubt, if the above licence is granted, the Supplier shall provide the Authority with the source code for the NHS Community Edition within 7 days to enable it to make use of the licence.
Standard Licence Terms	N/A
Acceptance Testing	N/A
Contract Price	The price(s) to be paid by the Authority to the Suppliers for the provision of the Services, as set out in the Call-Off ITT Response and reproduced at Annex 3.
Financial Model	The Suppliers' Financial Model, submitted if required by the Authority in the Supplier's Call-Off ITT Response and reproduced at Annex 3.

<table>
<tr><td>Contract Price for the purposes of Clause 19 (Limitation of Liability)</td><td>The price(s) to be paid by the Authority to the Suppliers for the provision of the Services, as set out in the Call-Off ITT Response and reproduced at Annex 3.</td></tr>
<tr><td>Guarantee</td><td>Not Applicable</td></tr>
<tr><td>Guarantee in favour of NHSE</td><td>Not Applicable</td></tr>
<tr><td>Payment Provisions</td><td>The payment terms for the payment by the Authority to the Suppliers of the Contract Price for the Services, as set out in the Call-Off ITT and reproduced at Annex 3; and

The level of reimbursement by the Suppliers to the Authority relating to any service credits in respect of failures by the Suppliers to meet the KPIs, as set out in the Call-Off ITT and reproduced at Annex 3.</td></tr>
<tr><td>Contract Managers</td><td><table><tr><td>Authority’s Contract Manager</td><td>Elaine Yip – Programme Manager</td></tr><tr><td>Supplier’s Contract Manager(s)</td><td>Michael Catania – SRO / Chief Commercial Officer</td></tr></table></td></tr>
<tr><td>Lead Contract Manager (if applicable)</td><td>Insert the Lead Contract Manager at the commencement of this Contract<table><tr><td>Supplier’s Lead Contract Manager</td><td>Michael Catania – SRO / Chief Commercial Officer</td></tr></table></td></tr>
<tr><td>Contract Meetings</td><td>The Supplier will be expected to attend weekly / fortnightly progress meetings with NHS England and NHS Improvement, and other relevant stakeholders, and attend Boards where relevant/required.</td></tr>
<tr><td>Fast-track Change values</td><td>N/A</td></tr>
</table>

Contract Reports – additional information	Not used
Person(s) to receive notices under the Contract	

Authority's nominated person and contact details for service of notices	Angela Maragna a.maragna@nhs.net Elaine Yip elaine.yip2@nhs.net
Supplier's nominated person and contact details for service of notices	Jill De Bene Jill.debene@sitekit.co.uk Michael Catania Michael.catania@sitekit.co.uk

Signed by the authorised representative of each AUTHORITY (as applicable)

Name:	Adrian Snarr	Signature:	
Position:	Director of Financial Control	Date	

Signed by the authorised representative of each of the SUPPLIERS

DocuSigned by:
Adrian Snarr
17F29B60E0CF430...

Name:	Jill de Bene Full Name: adrian snarr	Signature	…… ……
Position:	CEO Job Title/Role: director of financial control		
(Insert an additional signature block for each co-bidder)	Date Signed: 21/6/22		

Order Form Annexes

Annex 1

Part 1: Specification

Part 2: KPI Overview

Part 3: KPIs

Part 4: Calculation of Service Credits

Part 5: Termination Trigger for Accrued KPI Failures

Part 6: Excusing Events

Annex 2

Extra Key Provisions

Annex 3

Contract Price and Payment Terms

Maximum Payments on Unilateral Termination

Supplier's Financial Model

Annex 4

Implementation Plan

Annex 5

Information Security Management Plan

Annex 6

Supplier Solution

Annex 7

Processing of Personal Data

Annex 8

Acceptance Testing

Annex 1

Part 1: Specification
NHS Digital Staff Passport Service

Scope of this procurement

1. This tender is associated with the commitment in the NHS People Plan to streamline induction and onboarding processes and to passport training and skills from previous employers and more recently with the Secretary of State's commitment to offer a digital staff passport for Doctors in Training (DiT) and other staff groups from March 2022.

2. The ambition is to provide a NHS Digital Staff Passport to improve staff's experience when the move from one NHS organisation to another, providing the new employer a digital, verified record of identity, previous employment and training. The NHS Digital Staff Passport comprises the following components:
    - **NHS Digital Staff Passport Service** – consisting of:
        - **Interoperable digital wallets and Verifiable Credentials ecosystems** – providing an interoperability layer referred to as the Wrapper SDK for discovery and interaction with approved digital wallet stacks and the licensing and support for use of these stacks. **As defined in this Order Form.**
        - **NHS Trusted Frameworks** – the official register(s) for the NHS Trusted Frameworks, including the technical trust framework, as well as the first trust frameworks for employment checks, core skills training and immunisation and vaccination records
    - **NHS Organisations Service – consisting of:**
        - **NHS Organisations Portal** - to issue verifiable credentials and verify credentials – this is being procured separately and in parallel.
        - **Adoption Service for NHS Organisations** – providing product and service management for NHS organisations and managed by NHSE&I.
    - **NHS Workforce Data and Interoperability Standards** – setting the standards for data to be transferred into and out of the digital staff passports as well as for other workforce systems.

3. The scope for this Order Form is to set up the NHS Digital Staff Passport Service which encompasses:

    a) Supply of licenses for use of digital wallets and VC ecosystems, including trust list and status list.
    b) Development and support for Wrapper SDK for interoperability with wallet stacks.
    c) Technical support service for selected digital wallet and VC ecosystems as defined by the SLA in Annex 1 Part
    d) Administration of trust registers for the trusted frameworks, revocation lists and other similar trust registers. Specifically, to add or remove issuers and credential schema as notified by the NHS. The development and adoption of Trusted Frameworks in not in the scope of this Order Form.
    e) Support the initial scope of permanent staff movements of Doctors in Training (DiT) employed by NHS organisations and for temporary staff movements for all staff employed by NHS organisations. The service will need to be scalable to cover all

permanent and temporary staff movements between NHS organisations and extensible to enable staff movement into and out of the NHS.

Lifecycle Information Flow Requirements

4. The required capabilities of a digital wallet and VC ecosystem solution are to support the lifecycle information flows for verifiable credentials, and operation of a verifiable data registry.

5. Required capabilities for lifecycle information flows:
   a) An issuer can issue a verifiable credential to a holder's digital wallet.
   b) A holder can present one or more of its verifiable credentials to a verifier, optionally inside a verifiable presentation.
   c) A verifier can verify the authenticity of the presented verifiable presentation and verifiable credentials. This should include checking the credential status for revocation of the verifiable credentials.
   d) An issuer might revoke a verifiable credential.
   e) A holder might delete a verifiable credential.
   f) A holder can store and manage multiple credentials from government, NHS, and other organisations.
6. Requirements for a verifiable data registry:
   a) An entity can register and maintain identifiers and associated public keys and supporting metadata to support proof mechanisms.
   b) An entity can resolve an identifier to discover the correct public keys and supporting metadata to validate a credential or presentation.
   c) An entity can register trusted issuers of credential types (within a registry or other trust scheme/list).
   d) An entity can discover whether an issuer of a credential is included in a registry or other trust scheme/list.

Technical and Security Requirements

7. The requirement is to enable an individual to use a digital wallet as a user agent to request, hold and present credentials that are cryptographically verifiable using the enabling public-key infrastructure (PKI) of a VC ecosystem as envisaged by the W3C Verifiable Credentials Data Model.

8. Specific wallet and VC ecosystem requirements include:
   a) Protect credentials, both when stored in a digital wallet solution and in transit, against unauthorised access and malicious attack.
   b) Ensure that authentication to access any digital wallet is at a level of trust at least as high as the highest trust credential held within that wallet.
   c) Provide functionality to protect keys, secrets and other private data (such as credentials) from unauthorised access or malicious attack.
   d) Include key management functionality to handle the generation, rotation, revocation, storage, signing, and protection of cryptographic keys and associated secrets.

e) Provide for point-to-point trust where a credential is presented to a Verifier.

f) Ensure credentials and their data payload for a subject are stored by a wallet on their mobile device and not in the cloud other than for backup purposes with the consent of the subject.

g) Enable a subject to present credentials issued to them without the risk of disintermediation.

h) Enable a subject to have granular control over the sharing of credentials. Subjects must have the ability to allow or deny the sharing of personal data at the point of request.

i) Provide a Backup and Recovery capability to protect Subjects in case of loss, corruption, or hacking of the Wallet solution.

j) Provide for the secure storage of the keys, secrets, and other private data that a subject elects to store in the wallet. The implementation of this secure storage may vary depending on the nature of the wallet but could be satisfied by: secure enclaves on mobile phones, or secure storage governed by trusted execution environments (TEEs).

k) Ensure the integrity of all messages exchanged between entities either at the network level or where personal or sensitive data is passed (e.g. in the form of a credential data payload) by digitally signing the data payloads. As all credentials in the trust framework should conform to the Verifiable Credentials Data Model this will be accomplished by digitally signing the credential payload on issuance of the credential.

l) Protect the privacy of the subject throughout the identity lifecycle. The principles of Privacy by Design and Data Minimisation should be observed as should the spirit of GDPR even if that Regulation is not enforced by law for a particular implementation.

Interoperability Requirements

9. An important requirement is choice of digital wallets and VC ecosystems whilst recognising wallet providers have adopted different protocols for the exchange of credentials.

10. Through market engagement the NHS has learnt about a Handshake Protocol that enables an issuer or verifier to determine which wallet and protocol are being used.

11. The requirement is for development of a component that implements Protocol Discovery and which can be released to issuers and verifiers as a SDK wrapper. The initial protocols to be supported are the DIDComm and SIOP protocols. The SDK wrapper should be extensible to include other protocols over time. Providers are encouraged to propose alternative protocols where this has a strategic advantage for the NHS and for inclusion in future iterations of the ecosystem.

Support for Multiple Wallet Stacks: Verifier

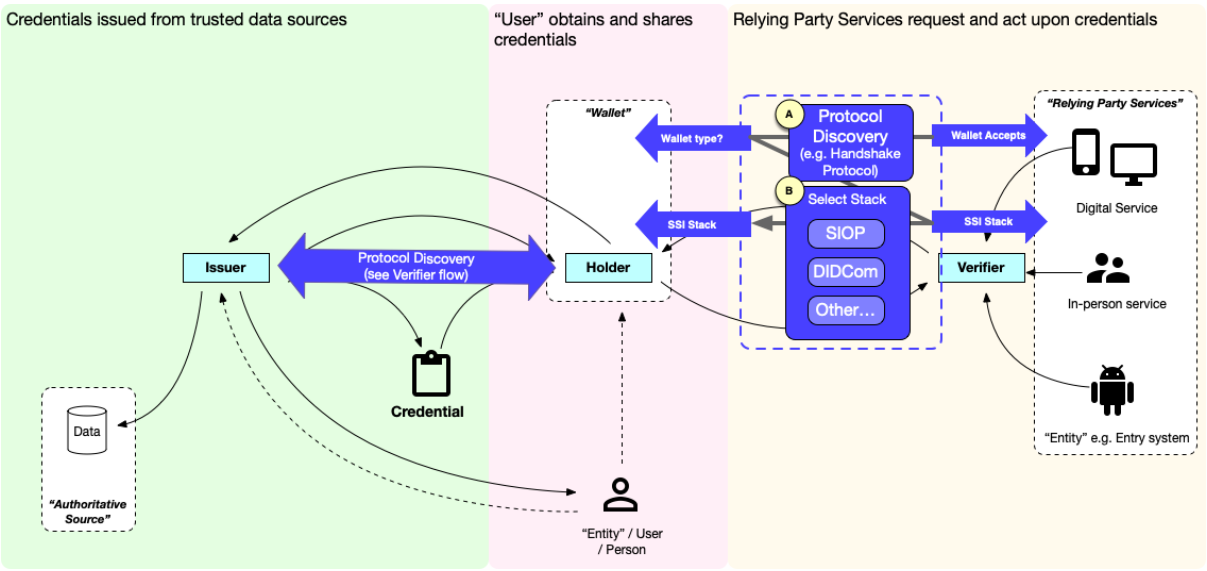


***Figure 1**: Wallet stack discovery overview*

12. To ensure that multiple wallet providers can be supported the requirement is for a capability for Protocol Discovery whenever communication between another entity and the Subject's Wallet is initiated.
13. A proposed solution for the Handshake Protocol is outlined in Figure 1, where Protocol Discovery would occur in 2 steps:
    a) The request is initiated by an entity such as a Verifier in the form of a standardised QR code. The Wallet responds to this request by identifying the SSI Stack to which it conforms.
    b) The requesting entity receives the response from the Wallet and reissues the request in the correct form (as dictated by the Wallet's SSI Stack preference).

Support for Multiple Wallet Stacks: Issuer

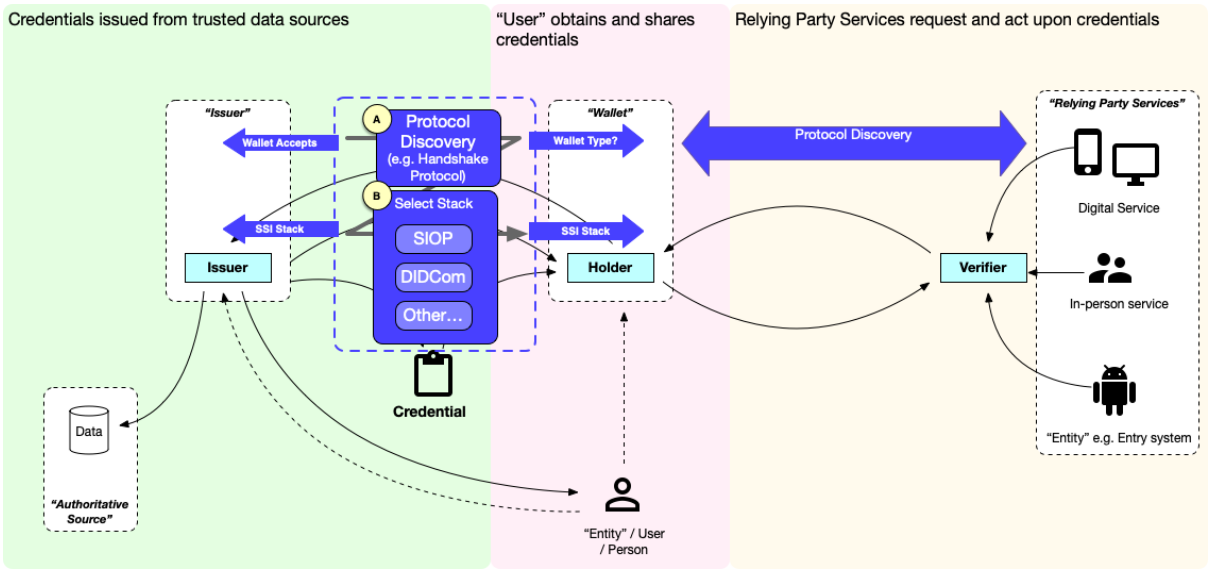


Figure 2: Wallet stack discovery during Issuance

14. As described above for protocol discovery with Verifiers, implementors are also encouraged to support protocol discovery for communication between Issuers and Holders / Wallets when offering and accepting verifiable credentials.
15. Similarly, to the proposed solution for interoperability between wallets and Verifiers, Protocol Discovery between Issuers and Holders / Wallets should follow the Handshake Protocol. The discovery process would therefore occur in 2 steps:
    a) The request is initiated by an entity such as an Issuer in the form of a standardised QR code. the Wallet responds to this request by identifying the SSI Stack to which it conforms.
    b) The requesting entity receives the response from the Wallet and reissues the request in the correct form (as dictated by the Wallet's SSI Stack preference).

Ensuring selection of an appropriate SSI stack for the Wallet

16. To enable discovery of the SSI stack required for interaction with a Wallet, the Issuer or Verifier should present an initial QR code (for scanning by the user device and Wallet) that includes a short URI that points to a requester based on the SIOP standard of abstracting the request into a URI.

    https://openid.net/specs/openid-connect-core-1_0.html#RequestUriParameter

    Example request

    ```
    openid://?request_uri=[uri_to_full_request]
    ```

    Taking this approach, the Wallet may then query for the full request and at the same time identify the SSI stack required.

    When making a request to the URI, the wallet adds `accept` to the http request header to identify itself.

```
Accept = #( media-range [ accept-params ] )
```

Example:

```
Accept = application/json
```

As a minimum the SIOP and DIDComm SSI stacks should be supported for interoperability with Wallet providers. Other providers are encouraged to propose alternative stacks where this has a strategic advantage for the NHS.

Therefore, the initially accepted SSI stack responses would be as follows:

Protocol	**Example Wallet**	**mime type**
SIOP (Self-Issued OpenID Connect Provider)	Authenticator	application/jwt
DIDComm	Connect.me	application/json

Ensuring Wallets identify themselves fully to Issuers and Verifiers

17. As part of Protocol Discovery, Issuers and Verifiers should include a URL in QR codes initially presented to Wallets.

    When responding to this URL to inform the Issuer or Verifier of which SSI stack to use for subsequent communication, Wallets should also include in the HTTP request `User-Agent`[1] to identify the Wallet product and version.

    Profiling the Handshake Protocol, requests to identify the wallet would identify the wallet with both `accept` and `User-Agent`:

    ```
    Accept = #( media-range [ accept-params ] )

    User-Agent = product *( RWS ( product / comment ) )
    ```

    Example:

    ```
    Accept: application/json

    User-Agent: connect.me/1.6.2.80455
    ```

    Wallet providers should ensure that their Wallet instances include a unique User-Agent when making requests to URLs presented by Issuers and Verifiers also in the trust framework.

Trust List and Issuer Discovery

18. An out-of-band list of trusted Issuers and the credentials is required for use by Verifiers. The entities on the trust list will be maintained and published by the NHS or a Trust

[1] User-Agent / RFC 7231 - https://datatracker.ietf.org/doc/html/rfc7231#section-5.5.3

Framework Operator appointed by the NHS. Each VC ecosystem is required to support an operational Trust List service.

Trusted Wallet List

19. An out-of-band list of trusted Wallet products and versions is required for use by Issuers and Verifiers. This trusted list will be maintained and published by the NHS or a Trust Framework Operator appointed by the NHS.
20. Issuers and Verifiers should not trust wallets that do not identify themselves as a product included in this trust list.

Workforce apps that include wallet functionality

21. The NHS is aware about the development of workforce related apps that include wallet functionality for the exchange of credentials. These apps will be considered as wallets that must comply with the requirements as specified in Annex 1.

Assurance Criteria

22. Each wallet and VC ecosystem is expected to provide evidence of meeting the following assurance requirements to the NHS or a Trust Framework Operator appointed by the NHS.

This draft list of assurance criteria will be refined during the alpha phase and evidence of meeting the criteria will form part of alpha assessment.

Code	Question	Options	Supporting information	Scoring criteria
C1.1	**Protection of Credentials**			
C1.1.1	Wallet providers: adequate protection of credentials	Provided | No evidence available		To pass, Wallet Providers must provide evidence of controls to ensure the protection of credentials, when stored in a digital wallet solution and in transit, against unauthorised access and malicious attack.
C1.1.2	Wallet providers: appropriate authentication for access to wallets	Provided | No evidence available		To pass, providers must provide evidence of authentication at an appropriate trust level is utilised when a Subject attempts to access data or functionality of the wallet solution. The level of authentication should be at a level of trust at least as high as the highest trust credential held within that wallet.
C1.1.3	Wallet providers: means of backup and recovery	Provided | No evidence available		To pass, providers must provide evidence of backup and recovery mechanisms that meet the highest level of trust supported by the framework.
C1.2	**Key Management / Security of Data**			
C1.2.1	Wallet providers: adequate protection for keys, secrets, and personal data	Provided | No evidence available		To pass, providers must provide evidence of implemented controls that protect keys, secrets, and other private data (such as credentials) from unauthorised access or malicious attack.

C1.2.2	Wallet providers: key management capability	Provided | No evidence available		To pass, providers must provide evidence of mechanisms for key management functionality to handle the generation, rotation, revocation, storage, signing, and protection of cryptographic keys and associated secrets. Providers should also describe the methods of key management and any scope limitations that may exist.
C1.2.3	Wallet providers: point-to-point trust	Provided | No evidence available		To pass, providers must provide evidence of implemented controls that ensure point-to-point trust where a credential is presented to a Verifier from the wallet.
C1.2.4	Wallet providers: digital signing of issuance and presentation requests, and presentation submissions	Provided | No evidence available		To pass, providers must provide evidence of the cryptographic techniques and profiles used for signing and their compliance with relevant standards such as FIPS 140-2.
C2	**Interoperability**			
C2.1	Please provide details of how your solution is able to interoperate with multiple wallet stacks as described in Annex 1 including a list of stacks supported.	Provided | No evidence available		To pass, the provider must evidence interoperability capability for the major digital wallet stacks e.g. SIOP and DIDComm.
C2.2	Please confirm that your solution conforms to the Protocol Discovery specification.	Yes | No | Not applicable		To pass, the provider must confirm that Protocol Discovery supported. If not applicable, the provider must provide a valid reason e.g. the solution is an Issuer only.
C2.3	Please confirm that your solution supports Presentation Requests either as a Verifier or as a Holder (wallet) processing such a request.	Yes | No | Not applicable		To pass, the provider must confirm that Presentation Requests are supported. If not applicable, the provider must provide a valid reason e.g. the solution is an Issuer only .
C2.4	Please confirm that a credential can be issued to a wallet in less than 5 seconds and a presentation can be verified in less than 5 seconds	Yes | No | Not applicable		To pass, the provider must evidence the performance for end to end issuance of a credential and end to end presentation and verification of a credential

Timeline

23. The expectation is for the Alpha to commence in February 2022 and for this initial testing phase to be concluded by the end of March 2022. The supplier will be expected to deliver the first iteration of the Alpha product for testing to commence no later than eight weeks into the project.
24. The expectation will be to progress to private Beta at the earliest opportunity once the most appropriate design and roadmap for implementation have been agreed based on the key findings from the Alpha. The private Beta will be expected to run until the end of December 2022.

Interdependencies/Other Workstreams

Trust/Trusted Frameworks

- For the solution to be successful for DiT and for temporary staff movements, the information held within the digital staff passport must be trusted by employers and individuals who will hold passport credentials, i.e., through agreement on what constitutes acceptable validation, and the security around personal data must be trusted by users through appropriate assurances on the security of the technology solution. To this end work NHSE&I has already commissioned work to define a technical trust framework scheme and to evolve the current NHS Employment Checks Standards and the Core Skills Training Framework into Trusted Framework scheme(s). NHSE&I and NHSX are working with Department of Digital, Culture, Media and Sport (DCMS) to ensure that these frameworks align with the UK digital identity trust framework.

Data Standards

- NHSX are in the process of defining the required data structure, governance, and assurance guidelines will need to be agreed, outlined, and put in place before a digital staff passport solution can be implemented.

Interoperability

- As a minimum, the digital staff passport must be able to accept data from the NHS Electronic Staff Records (ESR) operated by NHS Business Services Authority via the NHS Organisations Portal into the digital wallets provided by the NHS Digital Staff Passport Service and subsequently from Health Education England's Oriel and Trainee Information System (TIS) systems via the HEE Portal into the digital wallets provided by the NHS Digital Staff Passport Service. Both these portals are being developed under parallel procurement exercises, so the supplier chosen will be required to work with the respectively chosen suppliers and will be required to align their work as best as possible.

- NHSE&I is also leading work to interface occupational health and learning management systems into ESR, so that ESR will hold a full employment record. There is a potential that these systems could interface directly with the NHS Digital Staff Passport Service, in parallel or instead of ESR. The design for these interfaces will be defined in parallel with this Alpha project.

- NHSE&I and NHSX are working on the potential for interoperability of workforce systems to be handled through local 'exchange hubs' concept rather than via bi-lateral interfaces. Pilot projects for the first of type exchange hubs are underway and the designs of these will be considered alongside this project and the interface projects above.

- Piloting of the creation of verifiable credentials has already taken place with the General Medical Council (GMC) and they are keen to be involved in the Alpha phase, if possible. Discussions are underway with the Home Office and the DBS service regarding the potential to pilot their creation of right to work and DBS credentials. These projects may or may not align with the timings for the Alpha phase, although more likely align with private or public Beta phases.

- Consideration should be given on how to accept data from other 'passports' in the future which may be in use now or in the future.

Annex 1

Part 2: KPI Overview

Key Performance Indicators

1 During the Term of the Contract the Suppliers shall provide the Deliverables so as to meet the standard under each of the KPIs described below.

2 Annex 1 Part 3 of this Order Form sets out the Key Performance Indicators that the Parties have agreed shall be used to measure the performance of the Deliverables by the Suppliers.

3 The Suppliers shall monitor their performance against each KPI and shall send the Authority a report detailing the level of service actually achieved in accordance with the provisions of this Contract.

4 Subject to:

(a) any breach of any express provision of this Contract by the Authority (unless, and to the extent, caused or contributed to by the Suppliers); and

(b) any deliberate act or omission of the Authority or any failure by the Authority to take reasonable steps to carry out its activities in a manner which minimises significant interference with the Suppliers' performance of the Deliverables (save where, and to the extent, caused or contributed to by the Suppliers);

a failure by the Suppliers to meet any of the KPIs shall be KPI Failure (as defined in the Call-Off Terms and Conditions). Failure to meet a Primary KPI shall be a Primary KPI Failure and failure to meet a Secondary KPI shall be a Secondary KPI Failure.

5 KPI Failure Points, and therefore Service Credits, shall accrue for any KPI Failure. Service Credits shall be calculated in accordance with Annex 1 Part 4 of this Order Form

KPI Failure Points

6 If the level of performance of the Suppliers during a Measurement Period achieves the Target Performance Level in respect of a KPI, no KPI Failure Points shall accrue to the Suppliers in respect of that KPI.

7 If the level of performance of the Suppliers during a Measurement Period is below the Target Performance Level in respect of a KPI, KPI Failure Points shall accrue to the Suppliers in respect of that KPI as set out in Annex 1 Part 4 of this Order Form

8 The number of KPI Failure Points that shall accrue to the Suppliers in respect of a KPI Failure shall be the applicable number as set out in Annex 1 Part 3 of this Order Form depending on whether the KPI Failure is a minor KPI Failure, a serious KPI Failure or a severe KPI Failure as indicated in Annex 1 Part 3 of this Order Form, unless the KPI Failure is a Repeat KPI Failure when the provisions of Paragraphs 9 and 10 of this Annex1 Part 2 shall apply.

Repeat KPI Failures

Repeat KPI Failures

9 If a KPI Failure occurs in respect of the same KPI in any two consecutive Measurement Periods, the second and any subsequent such KPI Failure shall be a "Repeat KPI Failure".

10 The number of KPI Failure Points that shall accrue to the Suppliers in respect of a KPI Failure that is a Repeat KPI Failure shall be calculated as follows:

SP = P x 2

where:

SP = the number of KPI Failure Points that shall accrue for the Repeat KPI Failure;

and

P = the applicable number of KPI Failure Points for that KPI Failure as set out in Annex 1 Part 3 depending on whether the Repeat KPI Failure is a minor KPI Failure, a serious KPI Failure, a severe KPI Failure or a failure to meet the KPI service threshold.

Related KPI Failures

11 If any specific KPI refers to both Service Availability and System Response Times, the System Response Times achieved by the Supplier for any period of time during a Service Period during which the relevant Service or element of a Service is determined to be Non-Available shall not be taken into account in calculating the average System Response Times over the course of that Service Period. Accordingly, the Supplier shall not incur any Service Points for failure to meet System Response Times in circumstances where such failure is a result of, and the Supplier has already incurred Service Points for, the Service being Non-Available.

Annex 1

Part 3: KPIs

The KPIs are outlined as follows:

Key Performance	Metric	Measurement
Project Governance	Timely and accurate highlight reports detailing status, progress against timeline, dependencies, risks, issues and tracking against budget	• Weekly / fortnightly (TBC) reports
	Maintenance of roadmap and detailed workplan	• Weekly / fortnightly updated workplan
	Participation at regular stand ups and update meetings with SRO and team leadership	• Weekly / monthly attendance • Preparedness for meeting • Good input in update / discussions
	Attendance and presenting at regular governance meetings, including preparing papers in advance	• Attendance, as required • Preparedness for meeting • Quality of presentation materials
	Providing materials to aid senior decision-making	• Availability for ad hoc requests • Quality of material
Stakeholder management	Attendance and presenting at key stakeholder meetings, including preparing papers in advance	• Weekly / monthly attendance • Preparedness for meeting • Good input in update / discussions • Quality of materials
	Developing and maintaining relationships with key stakeholders	• Feedback from key stakeholders on the good relationship
Collaboration	Collaborative approach with NHS E&I team to ensure expertise and knowledge is shared	• Feedback from NHSE&I team on collaborative approach
Effectiveness	Delivery of Alpha within the agreed timelines and recommendations for delivery of the private Beta Successful completion of GDS and NHSX assurance criteria	• Agreed Alpha scope delivered within the agreed timelines • Preparation for GDS/NHSX service assessment and technical assurance • Clear recommendations for private Beta including: - Scope - Project plan - Costs - Roadmap and options for future scaling to other staff groups and bodies
Support	During Alpha phase acceptable support turnaround times for private Beta phase will be defined	• To be defined during alpha phase

Annex 1
Part 4: Calculation of Service Credits

Calculation of Service Credits – Primary KPIs

N/A

Consequences of accruing Secondary Failure Points

N/A

Annex 1

Part 5: Termination Trigger for Accrued KPI Failures

Termination for accrued KPI Failures

N/A

Annex 1

Part 6: Excusing Events

N/A

Annex 1

Part 7: SLA – Draft Service Level Agreement

1 Objectives

This agreement specifies the work delivered by Partner to Client comprising a Managed Service for the support of Digital Wallet and VC Ecosystem Infrastructure Applications that enable the day-to-day movement of staff using digital staff passports.

The Managed Service to include the deployment of software releases for specific Infrastructure Applications on a schedule agreed with the Client and following the agreed deployment process, in addition to notification and coordination of software releases by 3rd party digital wallet and VC ecosystem providers. This release schedule will reflect the operational needs of the service to support.

Client is NHS England and Improvement on behalf on the NHS organisations.
Partner is **Sitekit Applications Limited**.

This Service Level Agreement (SLA) is the baseline for the final SLA to be agreed between NHSE&I and Sitekit during this Contract.

2 Definitions

- “Managed Services” means a Contract between the Partner and the Client where it is specified what services are to be provided by the Partner throughout the period of the Service Level Agreement;
- “Resolution” means the Supplier addressing the Support Request and returning the system to live operational use in accordance with any relevant software documentation;
- “SLA” means Service Level Agreement;
- “Scheduled Work” means work scheduled to begin two calendar months or later from Client sign-off of a Work Plan;
- “Service Hours” means UK hours: 09:00-17:00 Monday to Friday (including public holidays); note UK changes from GMT to British Summer Time in the summer months and reverts to GMT during the winter;
- “Service Levels” means the standard for the Partner’s performance of its obligations set out in this Service Level Agreement;
- “Support Request” means a request by a Client Authorised Representative to the Partner to perform Managed Services;
- “Start Date” means the date when Parties agree in writing the Managed Services should start;
- “Unscheduled Work” means work scheduled to begin less than two weeks from Client sign-off on a Work Plan;

- "Work Plan" means the detailed description of the Managed Services the Supplier is required to perform under this Agreement, which will detail as applicable:

3 Supported Services

Certain tasks shall be carried out by the Help Desk in relation to Support Requests:

- Second line support of Client Authorised Representatives;
- Support of Staff Members who raise requests using a feedback feature within the selected digital wallets;
- Initial diagnostic identification, analysis and verification;
- Triage and re-assignment to partner organisation for resolution as appropriate;
- Provision of Support Request resolution as appropriate;
- Logging support calls and emails with the Help Desk as appropriate;
- Following incidents through from initial notification through to resolution;
- Communication of Support Request resolution to the Client Authorised Representative.

4 Service Scope

4.1 Core Services

The components of the core services comprise the support components of the Infrastructure Applications and are as follows:

a) Selected Digital Wallets: *tbd*
b) Selected VC Ecosystem Infrastructure Applications, including organisation SDKs: *tbd*
c) Wrapper SDK for interoperability with different wallet stacks

4.2 Maintenance Releases

Where necessary, maintenance releases of the software by the code provider will be issued to maintain compatibility with currently supported versions of third-party software. Such maintenance releases shall be deployed in line with Client Change Management. This may be varied by mutual agreement between the Parties.

4.3 Scheduled Maintenance

The Partner will make all reasonable endeavours to co-ordinate and restrict planned maintenance to a defined maintenance window this will be agreed with Client in advance. Some downtime may be unavoidable during this window, but The Partner will make every effort to minimise this. All such releases shall be deployed in line with Client Change Management, with the expectation that most releases will happen outside of working hours.

4.4 Help Desk

The IT Service Management system utilised as part of this service will be the Partner's ticketing system.

4.4.1 Contacting Helpdesk

The Help Desk shall provide a structured approach to raising Service Requests, Incidents and Problems via the internet and the following shall apply:

- All severity Level 1 and 2 incidents should be notified in an email to *tbd*
- All Service Requests, Incidents and Problems will be deemed to have been received at the time the Partner acknowledge receipt of the issue

4.5 Service Levels

Proactive maintenance, monitoring and network management shall maximise the reliability and availability of the Service.

4.5.1 Availability

Downtime will be minimised through discussions with Client with the aim for less than 45 minutes per month of unplanned downtime, excluding issues caused by upstream service providers and minus any periods of agreed Scheduled Maintenance.

Any service outage due to operational error or action on the part of the Customer (or any third-party that has been granted delegated operational management authority for the infrastructure) will be discounted from this calculation.

4.5.2 Level Definition & Prioritisation

The Partner shall provide a means by which Customer and Partner Authorised Representatives may raise Incidents on the Infrastructure Applications.

Service Requests, Incidents and Problems will be raised via the Partner's ticketing system, and resolution times will commence at the moment that the Incident is assigned.

Service Requests, Incidents and Problems will be deemed to have been received at the time the ticket was created. All Severity Level 1 and 2 incidents and problems will be passed to the Partner by the NHS Managed Service. As an additional step, the Partner will provide an email address *tbd* for P1s and P2s, which will trigger an alert for the on-call technician.

4.5.3 Resolution

Timescales

Resolution times will commence at the moment that an Incident is notified to the Partner.

All resolution timescales provided are calculated on a timer basis with the timer starting at the time the record is assigned to the Partner. When a Service Request, Incident or Problem is waiting on information or action from the Partner Authorised Representative, the timer is paused so as not to affect resolution timescales.

For example, with an 8 hour resolution timescale, whilst the Service Request, Incident or Problem is waiting on the Customer for response, the timer would not continue running

down. If a Service Request was issued 2 hours into an 8 hour resolution timescale, the timer would remain at 2 hours until a response from the customer had been received.

The list of examples in this section are not exhaustive. Where the Service Request, Incident or Problem raised cannot be described in the relevant table, the Severity Level shall be jointly agreed by the Partner Authorised Representative and the Partner.

The Partner will comply with all reasonable system access control and change control procedures of Client.

After any change to the Infrastructure Applications, the Partner shall inform the Partner Authorised Representative as soon as possible but fundamentally within 1 hour by an e-mail update or telephone depending on the level of severity. This update will confirm whether the change has been applied successfully and the result of any confidence tests carried out after the change.

4.5.4 Incidents

An Incident is defined as an unplanned interruption to an IT Service or reduction in the quality of an IT service.

Severity Level 1 and Level 2 Incidents raised during Service Hours shall be reported and a copy sent to *email address tbd*.

To ensure that the Partner's response is appropriate to the importance of the Incident, the concept of Level Definition shall be used. Where a P1 or P2 incident is raised there will be a response within 30 mins, and resolution will be identified. Note: the priority will be to get users accessing the system again as soon as possible, and where necessary an interim fix may be applied to facilitate this. It may be necessary to carry out further remedial work in the event an issue highlights a more significant problem.

The Partner will use best endeavours to facilitate the resolution times as outlined in this SLA, however it is not possible to guarantee every resolution can be achieved in this time due to the variable nature of potential issues and their complexity, and multiple partner solutions being in place. If a code change is required then this will be indicated to Client to advise on schedule and prioritisation of the release.

SEVERITY LEVEL	DEFINITION	INCIDENT RESOLUTION TIMESCALES
1 (Major Incident)	Complete loss of service at multiple sites.	In the event of a security breach, the technician will take immediate action to limit further unauthorised access to the Infrastructure Applications. Investigative work to provide a resolution will then commence during Service Hours • Response: 30 minutes • Resolution: 2 hours
2 (Major Incident)	Complete loss of service for all users at one site or partial loss of service at multiple sites.	• Response: 30 minutes • Resolution: 4 service hours
3	Partial loss of service for all users on one site.	• Response: 6 service hours • Resolution: Reasonable endeavours to obtain resolution in service hours equivalent to 1.5 days
4	Complete loss of service for some users on one site, OR partial loss of service for some users on one site, OR slow running on for any number of sites, OR any incident affecting a single user.	• Response: 1 service day • Resolution: Reasonable endeavours to obtain resolution in service hours equivalent to 4 days

4.5.5 Problems

A Problem is defined as the cause of one or more incidents.

Severity Level 1 and Level 2 Incidents raised during Service Hours shall be reported to *email address tbd*.

Please note: The priority will be to address the individual incident to ensure that normal service be resumed as soon as possible and not necessarily the underlying problem.

To ensure that the response is appropriate to the importance of the Problem, the concept of Level Definition shall be used.

SEVERITY LEVEL	DEFINITION	TIME TO IDENTIFY ROOT CAUSE
1	Consistent incidents are being raised that are causing the entire solution to become unavailable or are impacting data security.	• Response: 2 service days • IDENTIFY: 3 service days

SEVERITY LEVEL	DEFINITION	TIME TO IDENTIFY ROOT CAUSE
2	Consistent incidents are being raised that impact the availability of a critical module or component of the solution or make it unusable, impacting the vast majority of users.	• Response: 2 service days • IDENTIFY: 5 service days
3	Consistent incidents are being raised about an error or performance impact that significantly degrades the use of the solution for a small percentage of users.	• Response: 5 service days • IDENTIFY: Reasonable endeavours to identify root cause in service hours equivalent to 1 month
4	Consistent incidents are being raised about an error or performance impact that significantly degrades the use of the solution for a tiny percentage of users.	• Response: 5 service days • IDENTIFY: Reasonable endeavours to identify root cause in service hours equivalent to 2 months

4.5.6 Standard Changes

Changes to functionality are not covered by this agreement, but new releases that include new functionality agreed between Client and Partner will be covered by this agreement.

4.5.7 Scope of support – Supported items

Those listed under the definition of Infrastructure Applications during Service Hours for all Severity Levels.

4.5.8 Supported Services

Certain tasks shall be carried out by the Contractor in relation to Service Requests, Incidents and Problems:

- 2nd & 3rd line remote support of Customer or Partner Authorised Representatives
- Completion of Service Request, Incident or Problem resolution
- Communication of Service Request, Incident or Problem resolution to the Customer or Partner Authorised Representative

4.5.9 Excluded Services

The following are examples of services typically excluded from this SLA.

- Out-of-Hours support, i.e. 5pm – 9am UK Time
- Provision of on-site support or visits
- Supporting any functionality which is not part of the Infrastructure Applications

- Providing support as a substitute for training
- Issues caused by the disruption of upstream service providers
- Providing consultancy services (including making changes)
- Providing support for external applications
- Any amendments to the infrastructure not created by a member of the Partner or the selected Digital Wallets and VC Ecosystem providers.
- Resolution for bugs discovered or created before the commencement of this SLA. The implementation of fixes for pre-existing bugs should be covered in subsequent agreements.
- Breaking changes to the underlying Digital Staff Passport Portal platform are out of scope for this agreement, as these are considered issues with upstream providers.
    - In cases of breaking changes the Partner will diagnose the issue and advise Client.

4.5.10 Third-party code changes

Under the terms of this SLA the Partner will not be able to support infrastructure code changes by any party other than the Partner and the selected Digital Wallet and VC Ecosystem providers.

4.5.11 Service Request, Incident and Problem Closure

Where the resolution of a Service Request, Incident or Problem requires the Customer or Partner Authorised Representative to perform the testing then the Service Request, Incident or Problem shall only be resolved after the Contractor receives notification from the Customer or Partner Authorised Representative that the testing has been successful. Where notification is not received within 7 days, however, the Contractor reserves the right to close the Service Request, Incident or Problem.

The Contractor shall notify the relevant Customer or Partner Authorised Representative of any such closures. Should subsequent testing indicate the Service Request, Incident or Problem has not been resolved then the Service Request, Incident or Problem shall be reopened.

4.5.12 Recurring Incidents

Where an Incident of the same cause is raised repeatedly and a satisfactory, permanent resolution is not implemented (Problem), this shall be highlighted in the Service Level Report.

It should be noted that it may not always be possible to resolve an Incident particularly where it is dependent upon a third party. Should any such Incidents arise then they shall be highlighted.

4.5.13 Service Reporting

Upon request, the Partner shall report the following information on a monthly basis in the form of a Service Level Report:

- Services Requests, Incidents and Problems logged in the preceding 2 months, and the following information:
    - Unique tracking number
    - Description
    - Severity Level

    - Status
    - Resolution time frame (Where applicable)
- SLA Review
- Details of any changes required to be carried out
- Any exceptional events

4.5.14 Escalation

In the event that any item raised by Client should:

- Have a dispute surrounding the level allocated to the item
- Not be being progressed in the manner expected for the level
- Have exceeded or be very likely to exceed the SLA resolution times

The route that should be undertaken by Client to escalate should be in the order below, escalating to the next level only where opportunity has been provided and an adequate response has not been received.

1. Partner Service Desk Manager
2. Partner Service Director

The names of these contacts will be provided at the commencement of this agreement and any subsequent changes will also be informed to Client.

Escalation should be undertaken by phoning *tel no tbd* and asking for the relevant person.

Annex 2

Extra Key Provisions

The following words shall have the following meanings in Annex 3 of this Order Form and in the Call-off Terms and Conditions unless the context requires otherwise:

"Accepted"	Means in respect of any Milestone that that Milestone has been issued an Acceptance Certificate. "Acceptance" shall be construed accordingly
"Acceptance Certificate"	Means formal written confirmation issued by the Authority to the Suppliers that the Milestone has been approved by the designated Oversight Group
"Acceptance Criteria"	The criteria agreed between the Authority and Supplier which, if met, will lead to acceptance of the Milestones.
"Milestones"	Means those milestones as further described and set out at Annex 3 to this Call-Off Order Form. A Milestone is one of the Milestones.
"Milestone Date"	Means the target date by which the relevant Milestone is to be delivered as set out at Annex 3 to this Call-Off Order Form.
"Oversight Group"	Means the body responsible for approving the Milestone as set out at Annex 3 to this Call-Off Order Form.
"Remediation Notice"	Means a notice provided to the Supplier informing them that a Milestone has failed to be delivered in accordance with the Acceptance Criteria and providing the reasons for that failure.
"Remediation Period"	Means a period of 10 Business Days from receipt of the Remediation Notice, or such other period as agreed between the Parties.

Annex 3

Contract Price and Payment Terms

Contract Price

Total contract price: £690,000 (excluding VAT)

Alpha

Deliverable	Resource required	Cost (£)
Alpha - March - April		
Develop NHS Digital Staff Passport Wrapper SDK	*Resources stipulated in days, multi-disciplinary agile development teams with provision for*	

	PMO, security, development & testing.	
Migration of existing COVID-19 Digital Staff Passport onto Condatis Credential Gateway to support development of NHS Digital Staff Passport Portal, provision of end points and APIs for supplier of Digital Staff Passport Portal	[redacted]	
Feature prioritization of Condatis Credential Gateway (accelerated development of Condatis Credential Gateway features to support tender requirements, discounted to 30% of full build costs)		
Automation of onboarding organisations and credential configuration		
Updates to Trust List and Status List		
Post Office/Yoti Integration		
Onfido Integration		
Deeplinks		
Service provision through Alpha with minimal transactional volumes		
Condatis Credential Gateway		
Sitekit Support Wrapper		
Microsoft Azure AD Verifiable Credentials (nil cost, covered by NHS Azure Active Directory licenses)		
Evernym Verity 2.0 (nil cost, Evernym have agreed to reuse of licenses paid for by Sitekit under COVID-19 Digital Staff Passport contract)		

Private Beta

Deliverable	Resource required	Cost (£)
Release and manage NHS Digital Staff Passport Wrapper SDK until 31 December 2022, working jointly on several iterations with the supplier of the NHS Organisations Portal *(Note: discounted to reflect existing support arrangements between Sitekit and COVID-19 Digital Staff Passport team. Monthly charge under this contract of £27,625. Equivalent of 2 FTE throughout Beta period charged at £661.68 per day.*	[redacted]	
Service provision through private Beta until end of December 2022 with limited transactional volumes as follows:		
Circa 100 organisations and 1,000 passports by July 2022		
CondatisCredential Gateway (license & transaction)		
EvernymVerity2		
MicrosoftAADVC		
Circa 150 organisations and 5,000 passports by September 2022		
CondatisCredential Gateway (license & transaction)		
EvernymVerity2		
MicrosoftAADVC		
Circa 250 organisations and 50,000 passports by December 2022		
CondatisCredential Gateway (license & transaction)		
EvernymVerity2		
MicrosoftAADVC		

Contract Price for permitted extensions to the Term

Pricing will be held as proposed at the supplier's schedule of resource rates for the duration of any agreed extension/s.

Payment Provisions

Deliverable	Cost	Sub-total	Milestone	Estimated Invoice date
Alpha	[redacted]			
Develop NHS Digital Staff Passport Wrapper SDK				
Feature prioritisation of Condatis Gateway				
Automation of onboarding organisations and credential configuration				
Updates to Trust List and Status List				
Post Office / Yoti Integration				
Onfido Integration				
Deeplinks				
Service provision through Alpha with minimal transactional volumes				
Condatis Credential Gateway				
Sitekit Support Wrapper				
Microsoft Azure AD VC (covered by NHS Azure Active Directory license)				
Evernym Verity 2.0 (reused license under C-19 DSP contract)				
Sub-total for Alpha				
Private Beta				
Release and manage NHS DSP Wrapper SDK until 31 Dec 2022				
Service provision until end December 2021				
Condatis Credential Gateway (license and transaction) - 100 org, 1,000 passports				
Condatis Credential Gateway (license and transaction) - 150 org, 5,000 passports				
Condatis Credential Gateway (license and transaction) - 250 org, 5,000 passports				
Sub-total for Private Beta				

TOTAL CONTRACT VALUE		**£690,000**		

Note on subscriptions: each subscription (i.e. organisation) includes a limit of 100,000 credential exchanges per month. A credential exchange = a credential being issued or a credential being verified. If a subscription processes more than 100,000 credential exchanges within a month then an additional £100 will be billed to enable a further 1,000,000 credential exchanges within that month.

The payment profile for this Contract shall be payment per Milestone based on the completion of each Milestone. To be updated following contract award, based on milestones set by the Supplier.

Acceptance criteria for the approval of Milestones

1.1 At the relevant Milestone Date, the Authority shall assess the Milestone against the applicable Acceptance Criteria and in respect of each Milestone shall either:

- issue an Acceptance Certificate; or
- give notice to the Supplier that the Milestone has failed to be delivered in accordance with the Acceptance Criteria.

1.2 Where a Milestone fails to meet the applicable Acceptance Criteria, the Supplier shall use its best endeavours to re-perform such of its obligations as are necessary in order to bring such Milestone into conformity with the Acceptance Criteria during the Remediation Period or such other period as the Commissioner may propose in its Remediation Notice.

1.3 In the event of any dispute as to a decision of the Authority to issue a Remediation Notice or the Authority's reasons for determining that Acceptance Criteria have not been met, such dispute shall be referred to a relevant independent expert for determination.

Service Credits due in the event that Suppliers fail(s) to meet Milestone by Milestone date

In the event that the Supplier fails to meet any Milestone by the Milestone Date, the Authority shall be entitled to a Service Credit of 5% of the Contract Price for that Milestone for each full Month that the Deliverable is late.

In the event that the Supplier fails to meet any Milestone approval, the Authority shall be entitled to a Service Credit of 5% of the Contract Price for that Milestone for each occasion that the Milestone is presented to the Oversight Group and not approved.

Recovery of Service Credits in aggregate shall be limited to a maximum of 15% of the total Contract value.

Termination for failure to meet Milestone(s) by Milestone Date.

In the event that the Supplier fails to meet the Acceptance Criteria on 2 or more occasions for any single Milestone requirement the Authority shall have the right to terminate the Contract, or the part of the Contract in relation to that Milestone, with immediate effect from the date of issue of the relevant Remedial Notice.

In the event that the Supplier fails to meet the Acceptance Criteria upon first submission for any 3 Milestones, the Authority shall have the right to terminate the Contract with immediate effect from the date of rejection of the 3rd Milestone.

In the event that 2 or more Milestone Dates are missed, the Authority shall have the right to terminate the Contract with immediate effect.

Maximum Payments on Unilateral Termination by Authority

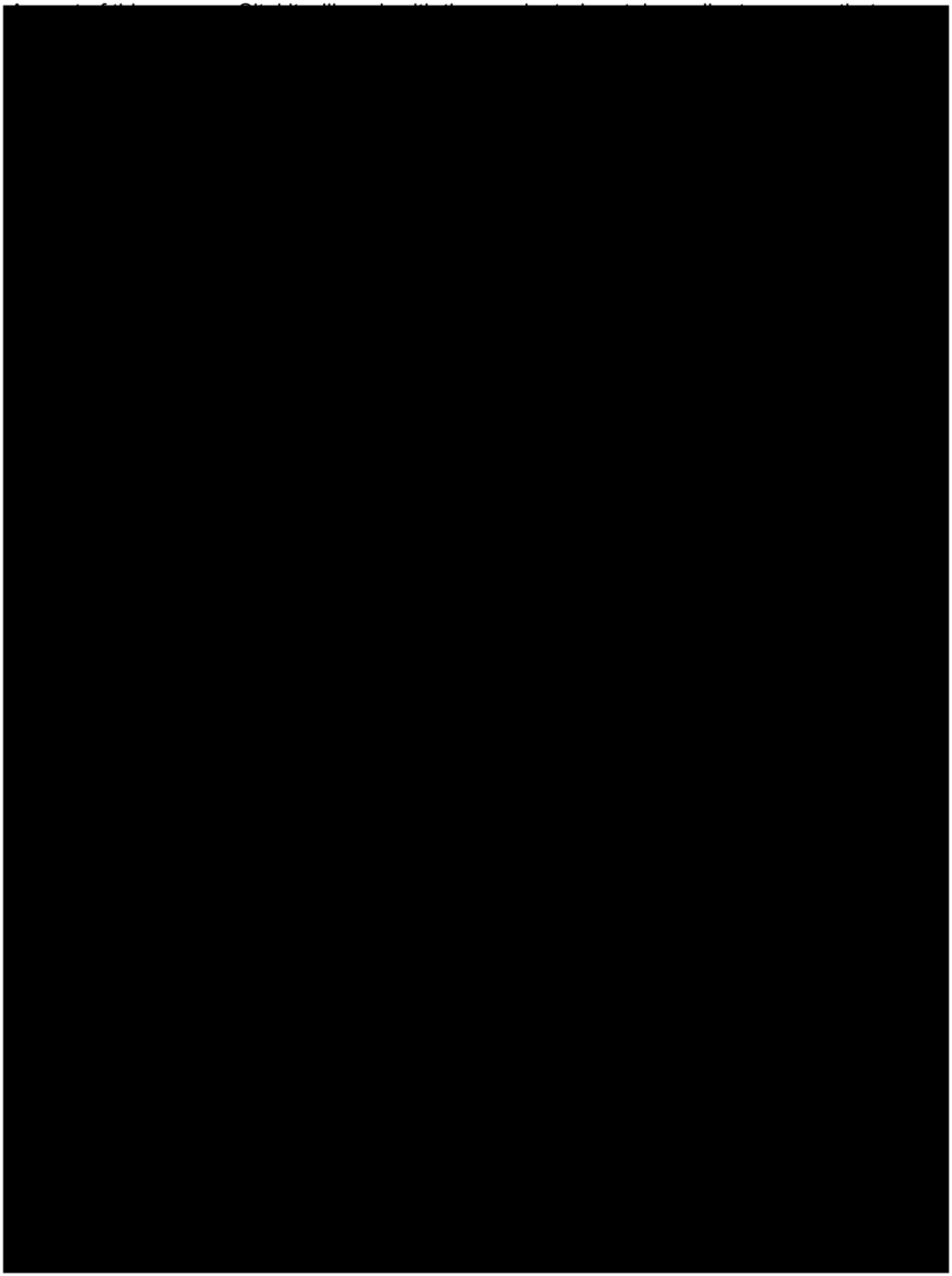
In-line with the awarded capped fixed price. Payment on invoice will be subject to the successful completion of deliverables as approved by the Authority's representative.

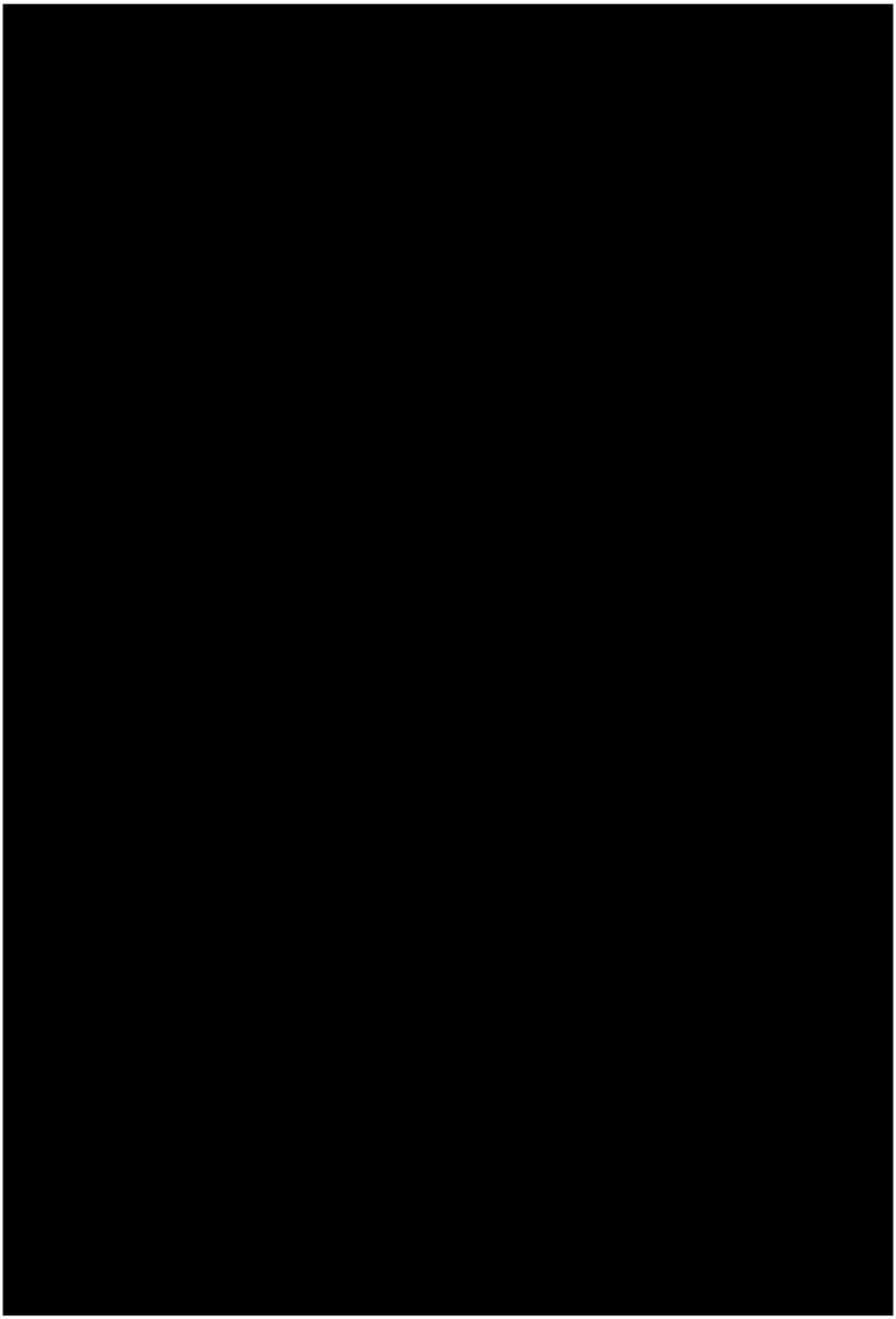
Annex 4

Implementation Plan

4.1 Alpha Phase Plan

[redacted]



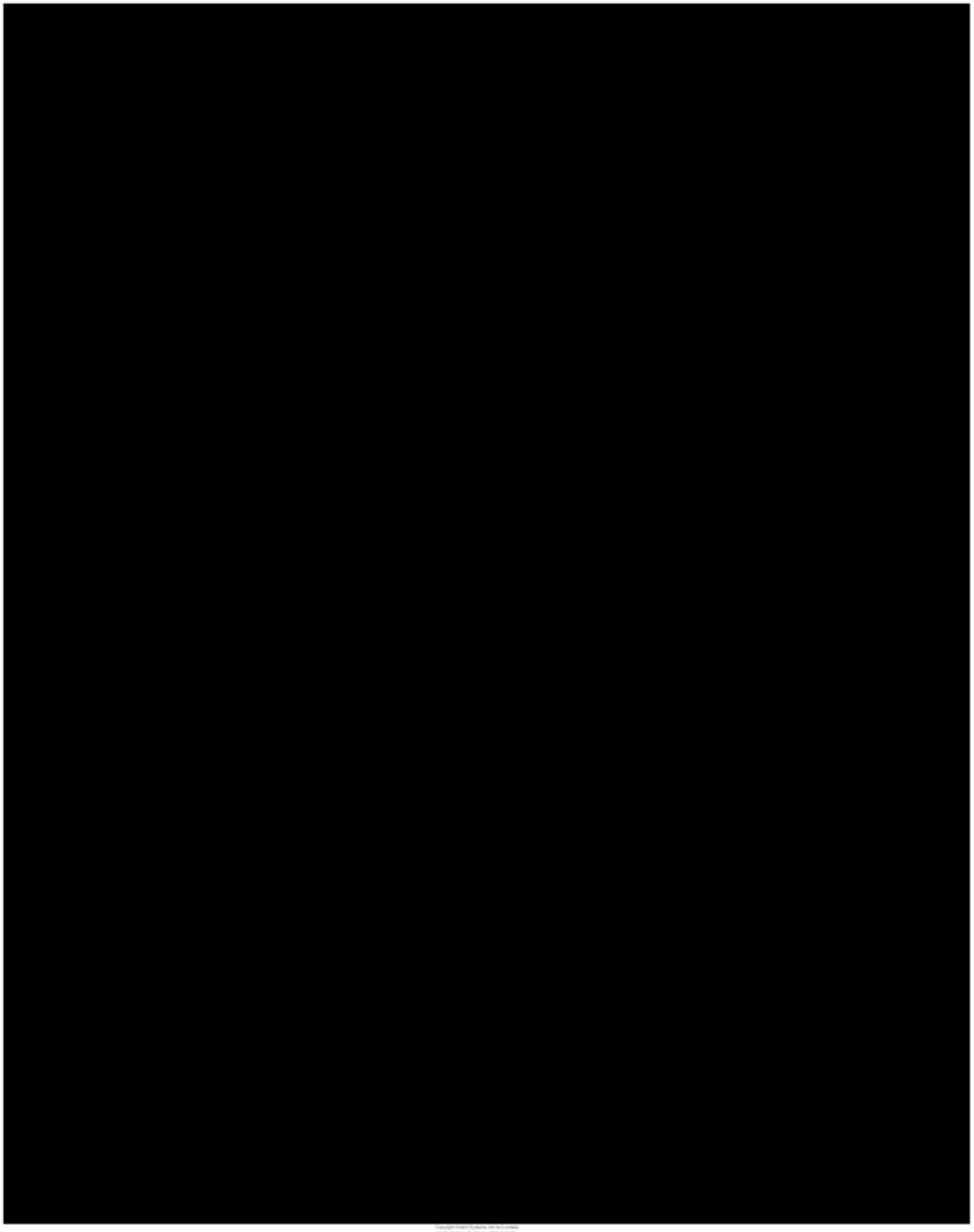


Annex 5

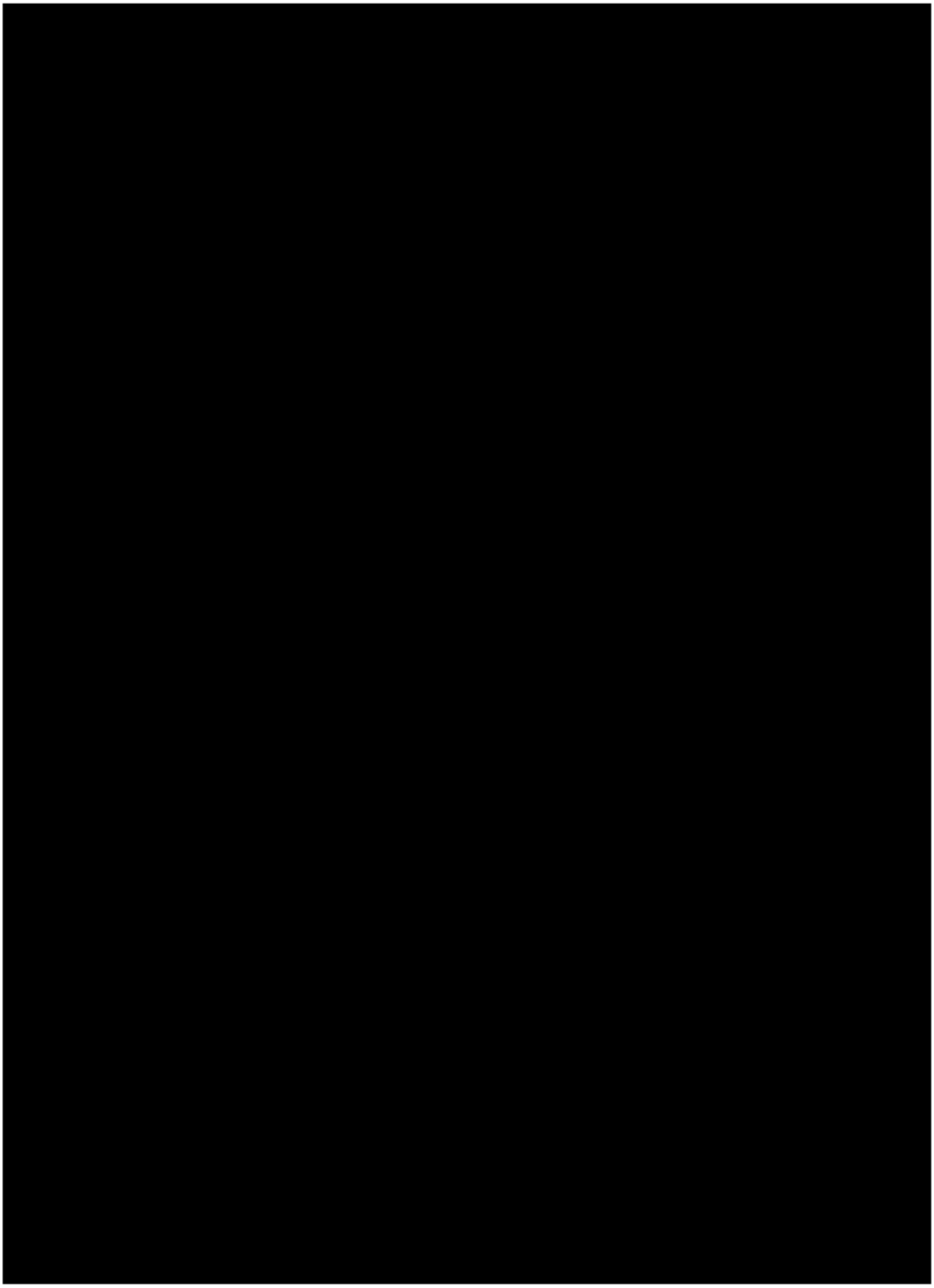
Information Security Management Plan

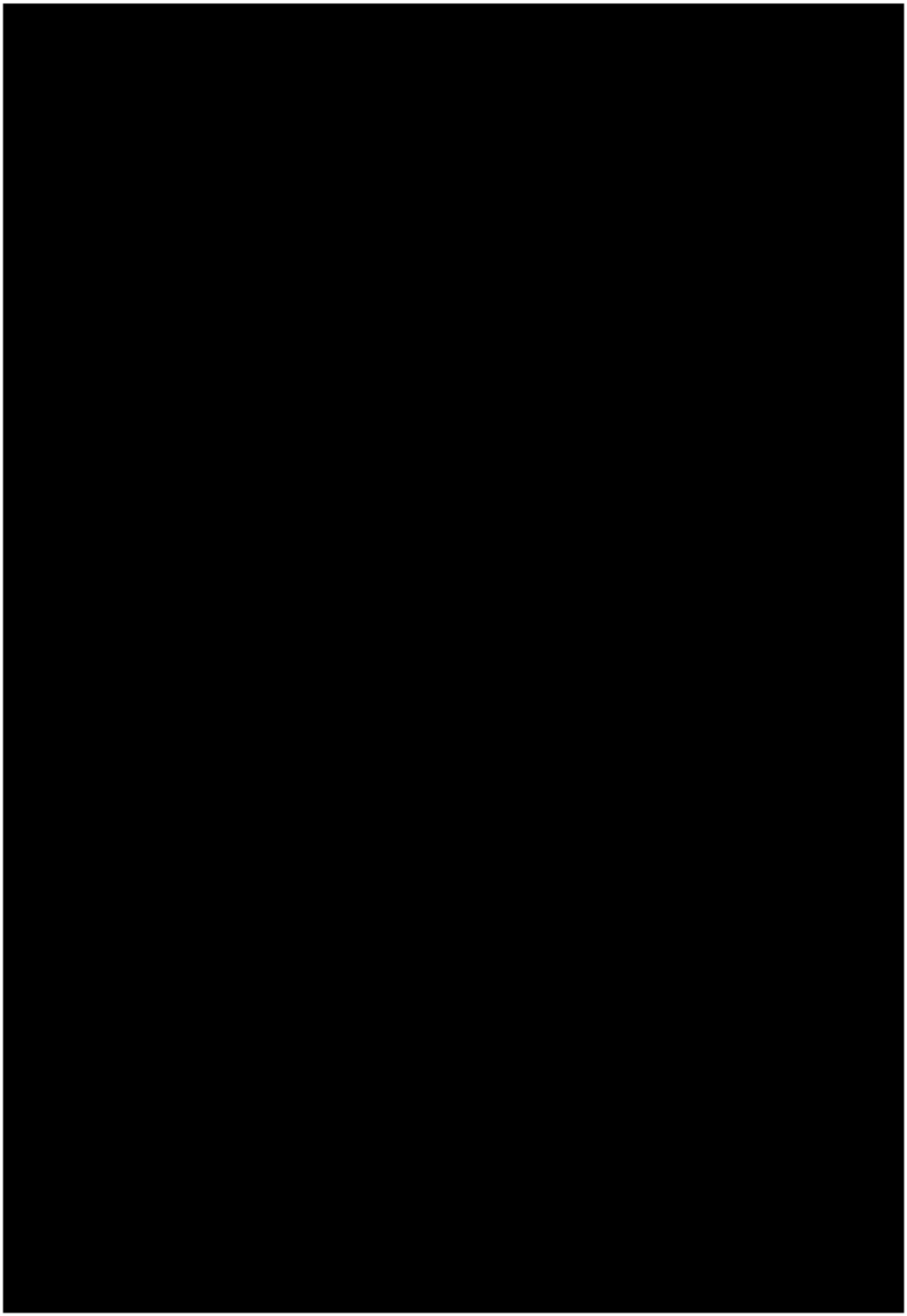
Annex 6

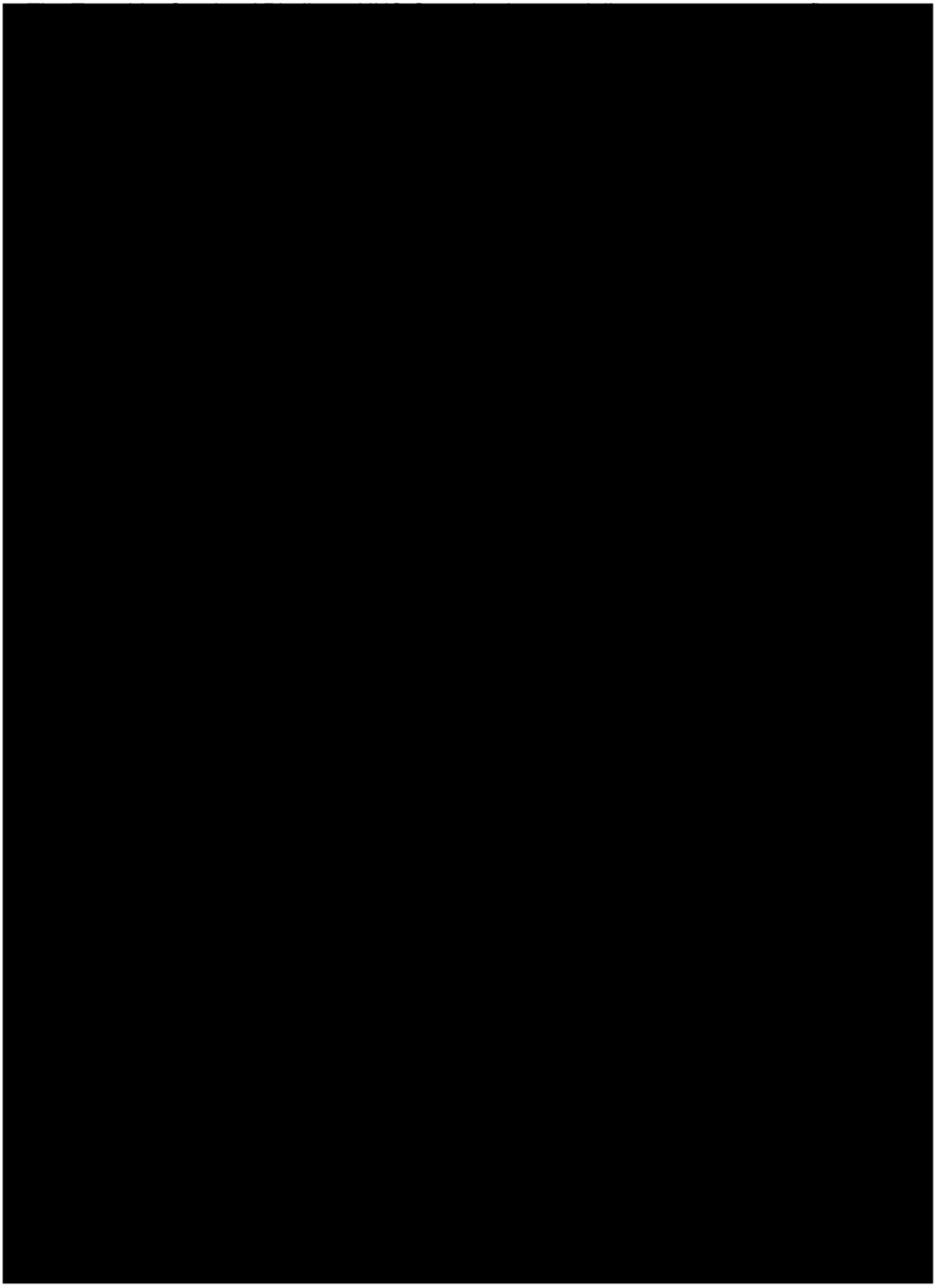
Supplier Solution

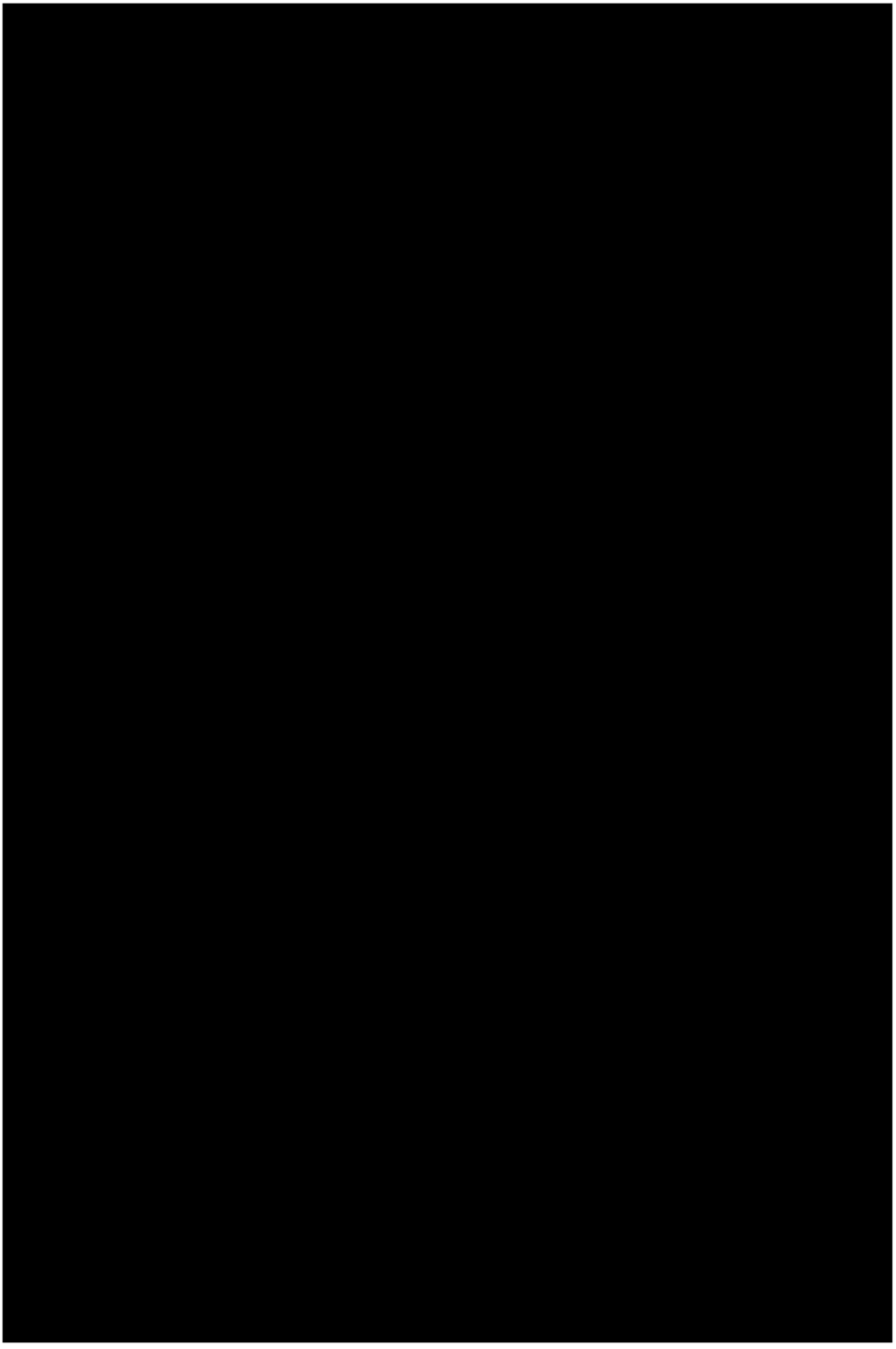


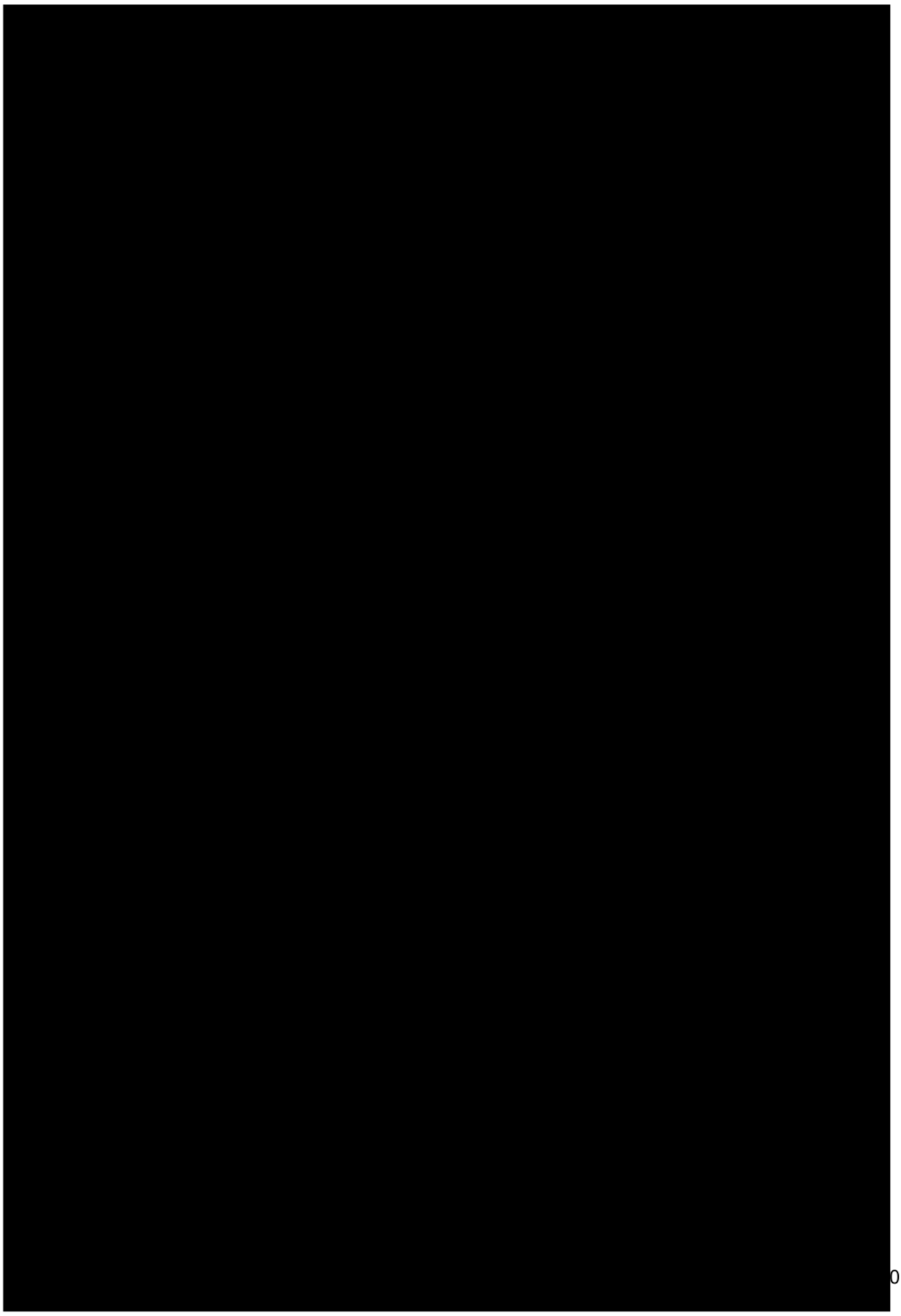
6.1.1. Component Description

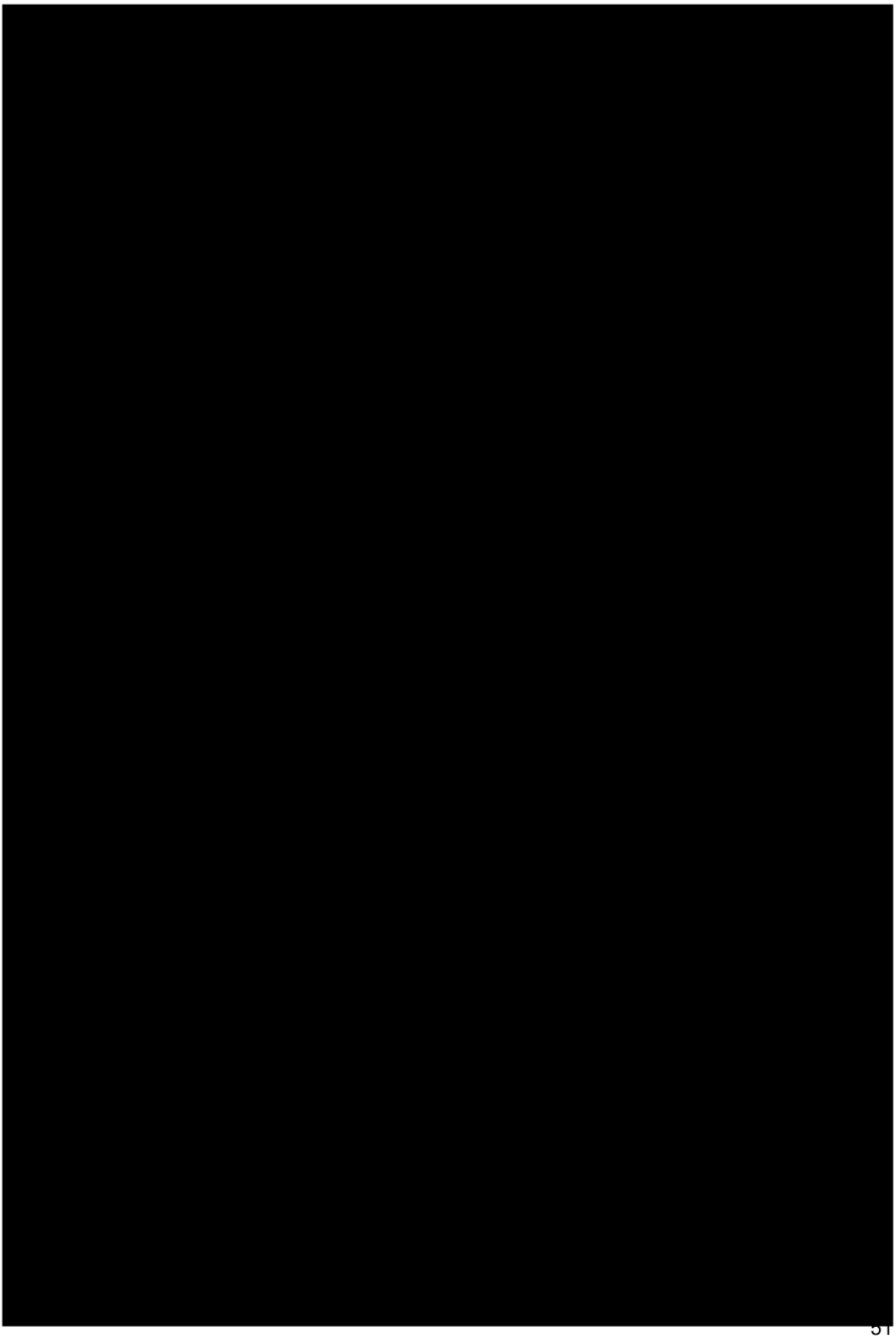


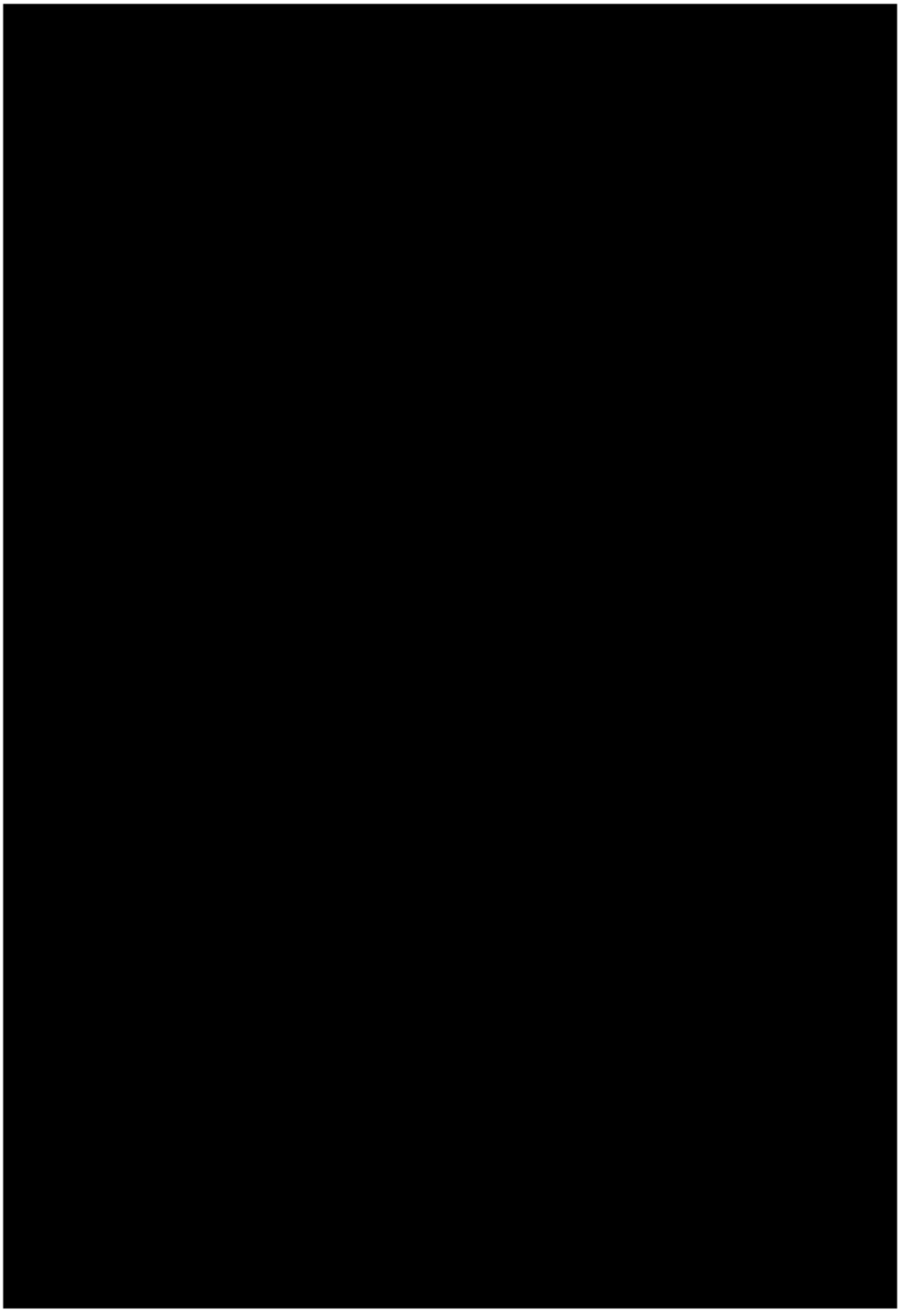




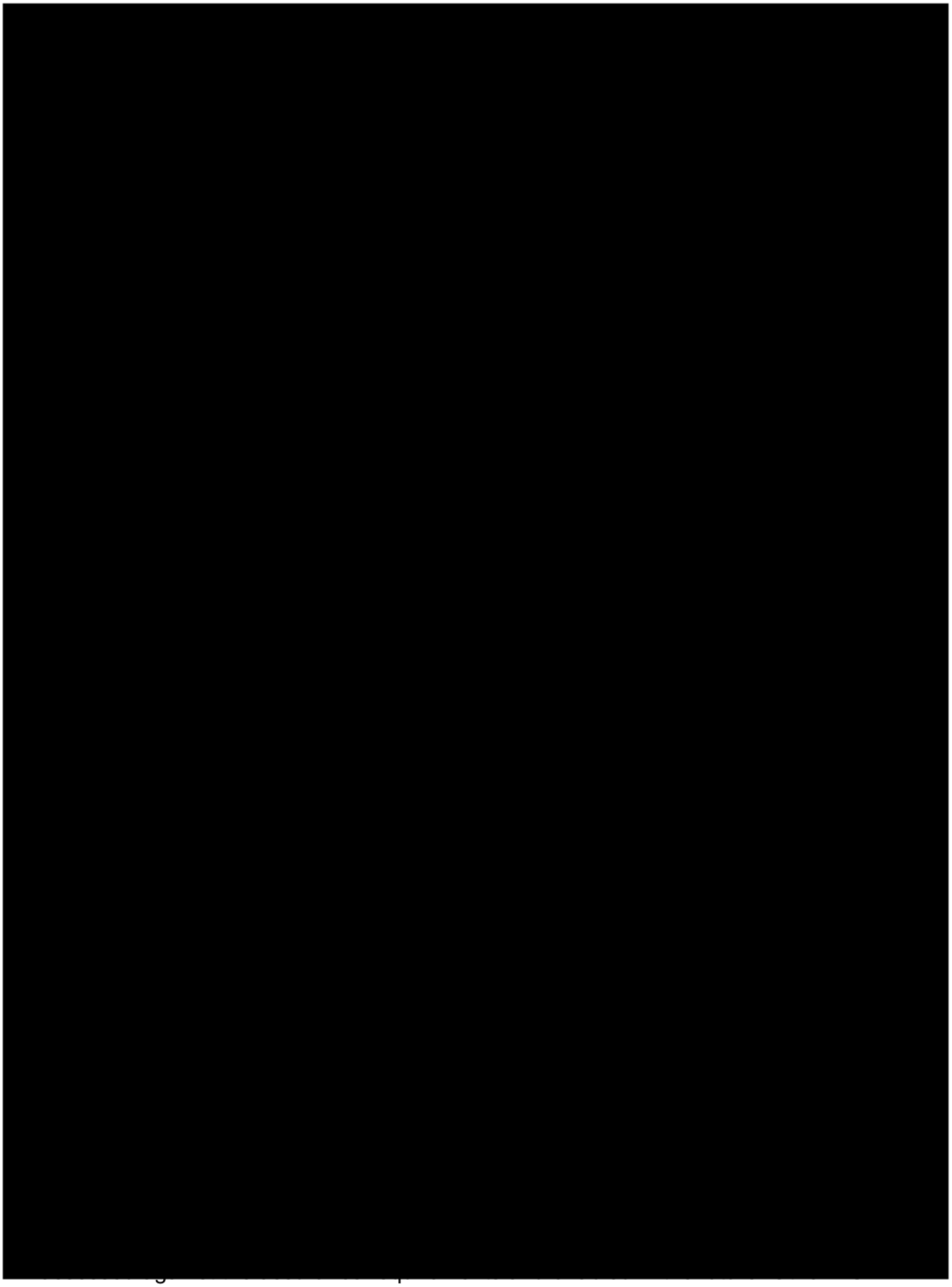


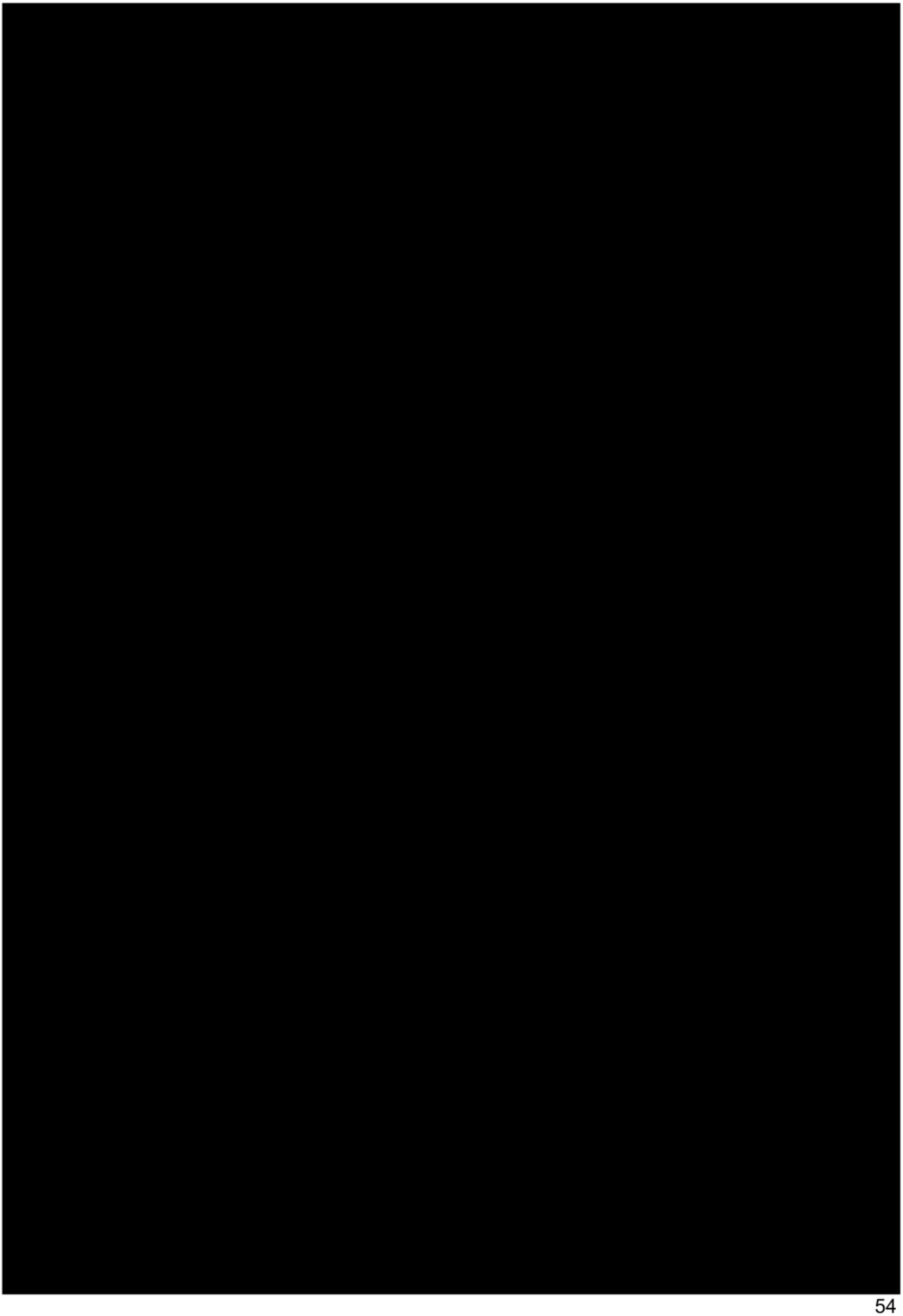


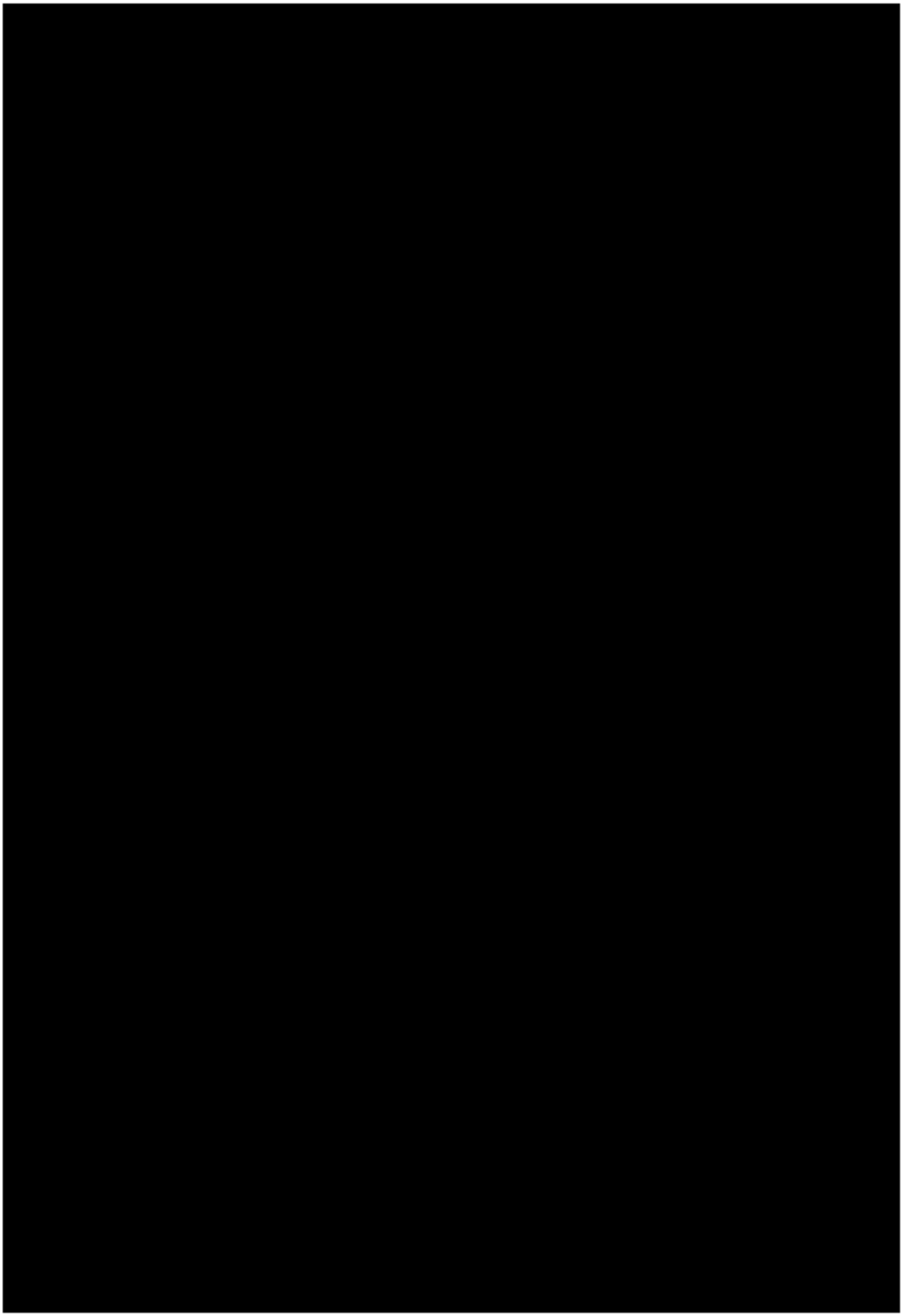


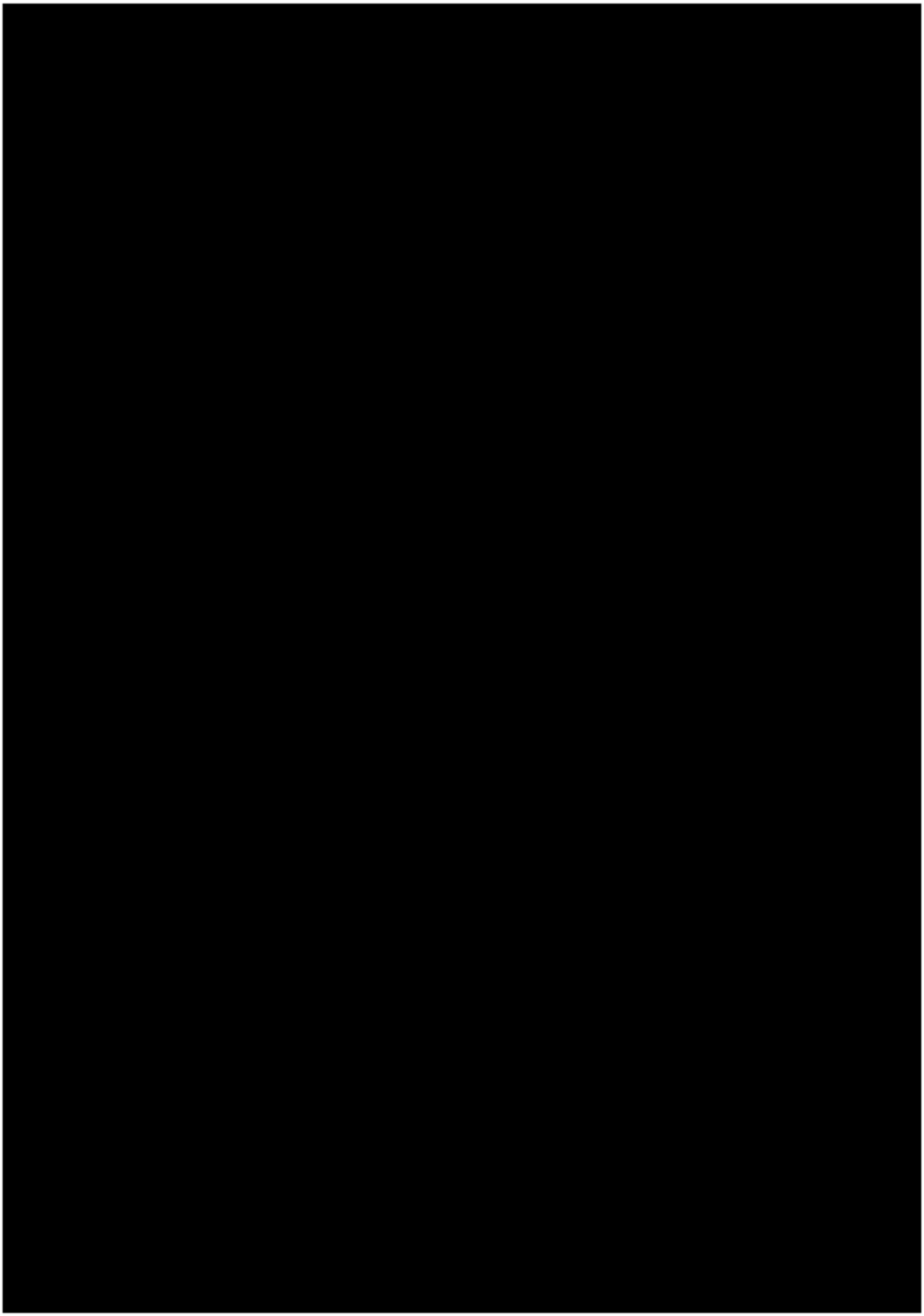


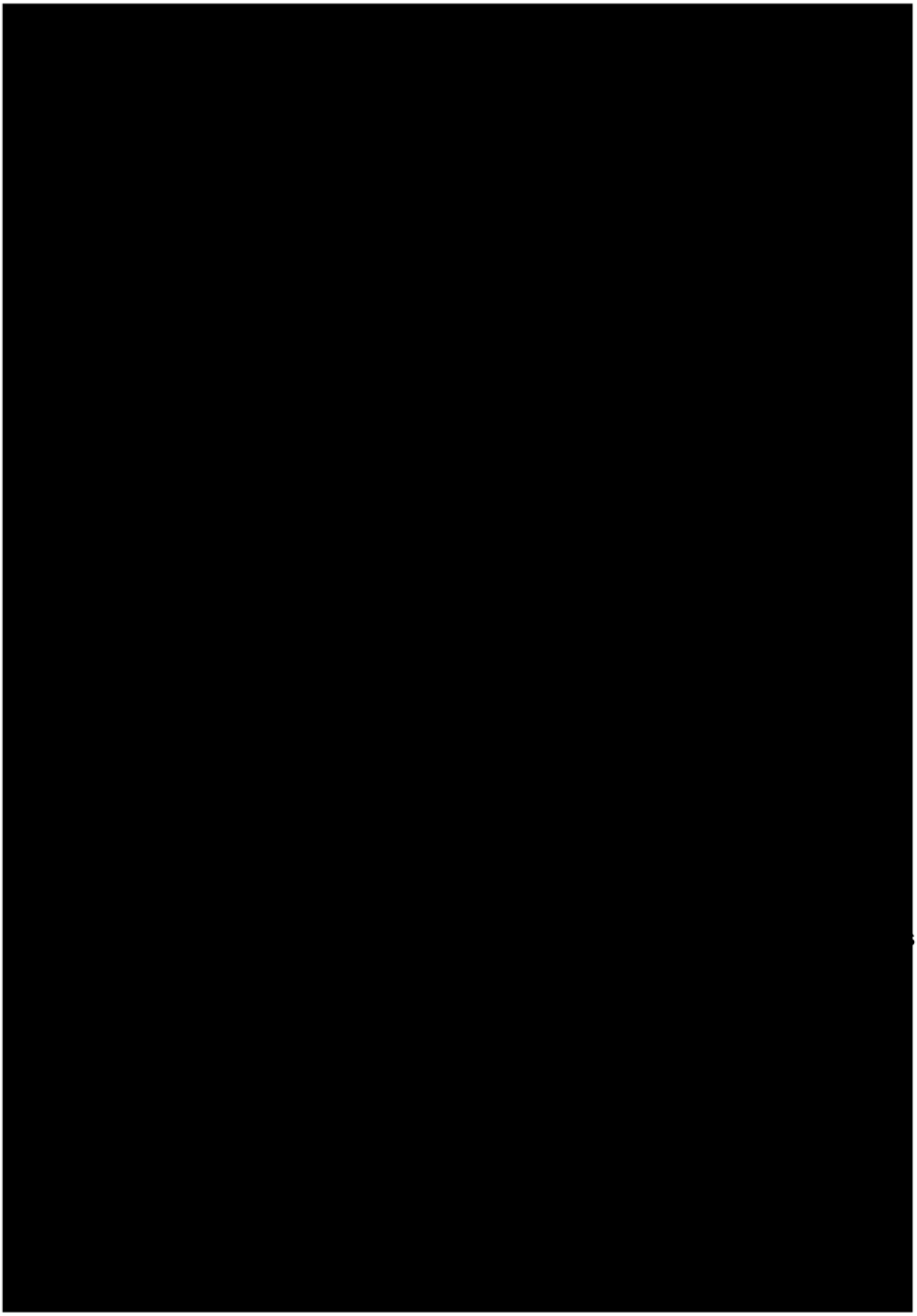
6.2.6. Description of how access to APIs will be protected



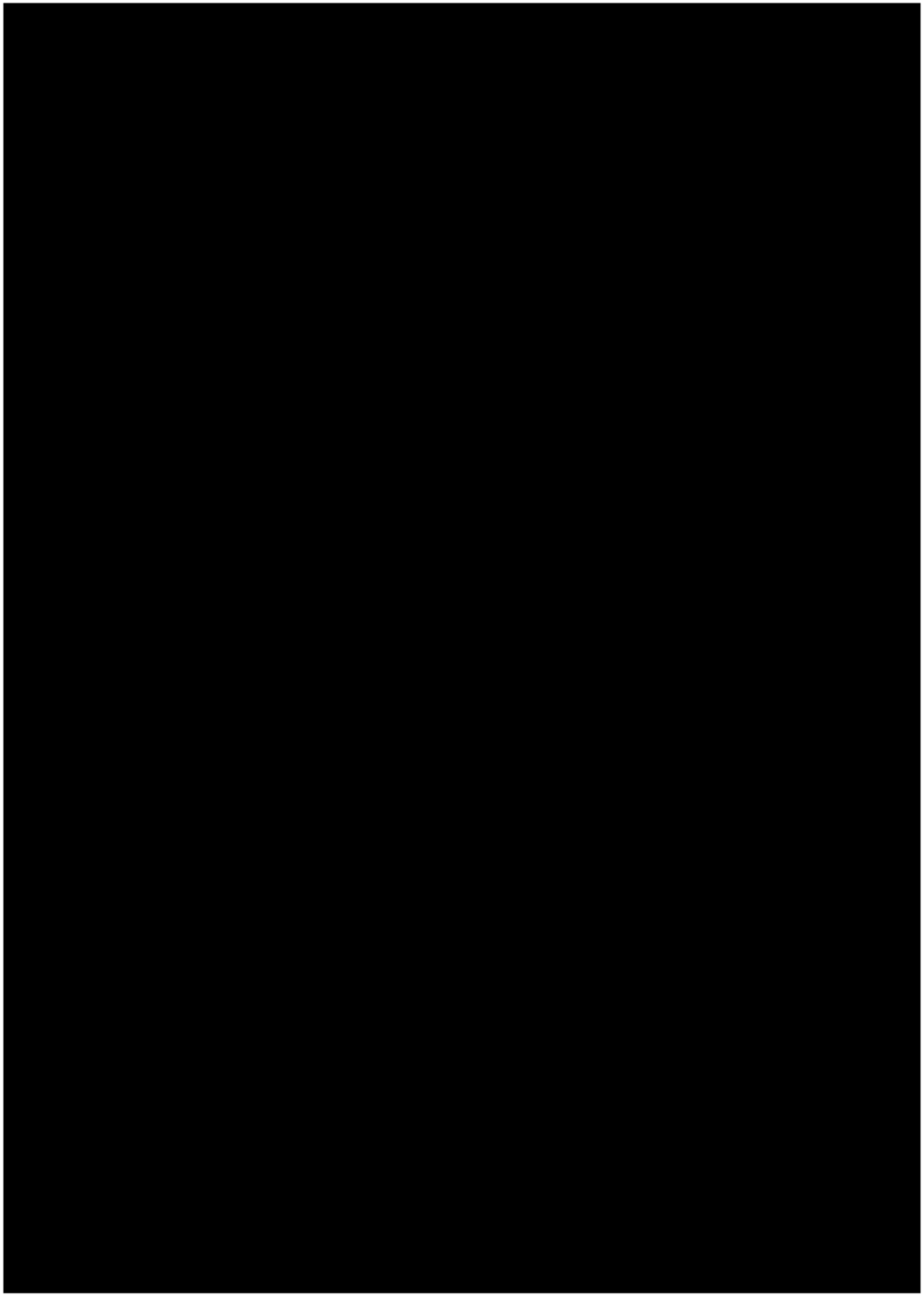








Sitekit Environmental Policies



Quality Management System Policies and Procedures. Support for diversity and inclusion within the workforce is a key objective for Sitekit as part of our Diverse Work Practices.

[redacted]

Annex 7

Processing of Personal Data

1. The Suppliers are only authorised to Process Personal Data in accordance with this Annex.
2. The Suppliers shall comply with any further written instructions with respect to Processing from the Authority from time to time.
3. Any such further instructions shall be incorporated into this Annex.

Annex 8

Acceptance Testing

NOT USED