



Technology Services 2 Agreement RM3804
Framework Schedule 4 - Annex 1

Order Form

In this Order Form, capitalised expressions shall have the meanings set out in Call Off Schedule 1 (Definitions), Framework Schedule 1 or the relevant Call Off Schedule in which that capitalised expression appears.

The Supplier shall provide the Services specified in this Order Form to the Customer on and subject to the terms of the Call Off Contract for the duration of the Call Off Period.

This Order Form should be used by Customers ordering Services under the Technology Services 2 Framework Agreement ref. RM3804 in accordance with the provisions of Framework Schedule 5.

The Call Off Terms, referred to throughout this document, are available from the Crown Commercial Service website <http://ccs-agreements.cabinetoffice.gov.uk/contracts/rm3804>

The Customer must provide a draft Order Form as part of the Further Competition Procedure.

Section A General information

This Order Form is issued in accordance with the provisions of the Technology Services 2 Framework Agreement RM3804.

Customer details

Customer organisation name

The Health and Social Care Information Centre known as NHS Digital

Billing address

Your organisation's billing address - please ensure you include a postcode

NHS Shared Business Services, T56 Payables A125, Phoenix House, NHS SBS, Topcliffe Lane, Tingley WF3 1WE

Customer representative name

The name of your point of contact for this Order

Dean Freed / Rob McMillan

Customer representative contact details

Email and telephone contact details for the Customer's representative

Always CC any correspondence to procmail@nhs.net

Supplier details

**Supplier name**

The Supplier organisation name, as it appears in the Framework Agreement
IBM United Kingdom Limited

Supplier address

Supplier's registered address
PO Box 41, North Harbour, Portsmouth, PO6 3AU

Supplier representative name

The name of the Supplier point of contact for this Order
[REDACTED]

Supplier representative contact details

Email and telephone contact details of the supplier's representative
[REDACTED]

Order reference number

A unique number provided by the supplier at the time of the Further Competition Procedure
Please provide the order reference number, this will be used in management information provided by suppliers to assist CCS with framework management

PRJ_4548

Section B

Overview of the requirement

Framework Lot under which this Order is being placed

Tick one box below as applicable (unless a cross-Lot Further Competition)

- | | |
|--|-------------------------------------|
| 1. TECHNOLOGY STRATEGY & SERVICES DESIGN | <input type="checkbox"/> |
| 2. TRANSITION & TRANSFORMATION | <input type="checkbox"/> |
| 3. OPERATIONAL SERVICES | |
| a: End User Services | <input type="checkbox"/> |
| b: Operational Management | <input type="checkbox"/> |
| c: Technical Management | <input type="checkbox"/> |
| d: Application and Data Management | <input type="checkbox"/> |
| 4. PROGRAMMES & LARGE PROJECTS | |
| (i) OFFICIAL | <input checked="" type="checkbox"/> |
| a. SECRET (& above) | <input type="checkbox"/> |

Customer project reference

Please provide the customer project reference number.

PRJ_4548

Call Off Commencement Date

The date on which the Call Off Contract is formed – this should be the date of the last signature on Section E of this Order Form

14/09/2020

Call Off Contract Period (Term)



A period which does not exceed the maximum durations specified per Lot below:

Call Off Initial Period Months

Call Off Commencement Date to
36 months from Go Live of the MVP.

Call Off Extension Period (Optional) Months

Up to 2 Call Off Extension Periods, each with a duration of up to 12 months. The Customer may extend the term of this Call Off Contract by giving the Supplier 30 days' written notice prior to the end of the Call Off Initial Period and the first Call Off Extension Period (where applicable).

Minimum Notice Period for exercise of Termination Without Cause 30

(Calendar days) *Insert right (see Call Off Clause 30.7)*

Additional specific standards or compliance requirements

Include any conformance or compliance requirements over and above the Standards (including those listed at paragraph 2.3 of Framework Schedule 2) which the Services must meet.

List below if applicable

With respect to Framework Schedule 2, the following standards shall be added as additional standards to paragraph 2.3.1(i) Information Security Management Standards:

- (ii) ISO 27001 Information Security Management Systems
- (iii) ISO 27002 Code of Practice for Information Security Controls
- (iv) ISO 27005 Information Security Risk Management
- (iii) ISO 27031 Guidelines for Information and Communication Technology Readiness for Business Continuity
- (iv) ISO 20000 Information Technology Service Management
- (v) ISO 22301 Business Continuity Management Systems

With respect to Framework Schedule 2, the following standards shall be added as additional standards to paragraph 2.3.1(e) Accessible IT Standards:

- (v) The NHS Digital Service Accessibility Standards and government guidance on making your service accessible to everyone that needs it:
 - a. <https://service-manual.nhs.uk/accessibility>
 - b. <https://www.gov.uk/service-manual/helping-people-to-use-your-service/making-your-service-accessible-an-introduction>
- (vi) Government Digital Services framework and the accessibility requirements of WCAG2.1 (meeting at least level AA) - <https://www.gov.uk/service-manual/helping-people-to-use-your-service/understanding-wcag>

With respect to Framework Schedule 2, the following standards shall be added as additional standards to paragraph 2.3(l) Miscellaneous:

- (vi) NCSC security recommendations - <https://www.ncsc.gov.uk/collection/cyber-security-design-principles>
- (vii) NIST cybersecurity standard recommendations - <https://www.nist.gov/cyberframework>



- (viii) GDS service standard - <https://www.gov.uk/service-manual/service-standard>
- (ix) NHS service standard - <https://service-manual.nhs.uk/service-standard>
- (x) Any clinical software build shall be compliant with the clinical risk management standards DCB0129 and DCB 0160 - <https://digital.nhs.uk/services/solution-assurance/the-clinical-safety-team/clinical-risk-management-standards>
- (xi) NHS Digital standards - <https://digital.nhs.uk/about-nhs-digital/our-work/nhs-digital-data-and-technology-standards/framework>
- (xii) Government Digital Standard and Password Guidance - <https://design-system.service.gov.uk/patterns/passwords/> and https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/458857/Password_guidance_-_simplifying_your_approach.pdf
- (xiii) NHS guidelines for cloud infrastructure - <https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/nhs-and-social-care-data-off-shoring-and-the-use-of-public-cloud-services/nhs-and-social-care-data-off-shoring-and-the-use-of-public-cloud-services-guidance>
- (xiv) The Business Continuity Institute Good Practice Guidelines - <https://www.thebci.org/training-qualifications/good-practice-guidelines.html>

The following table shall replace Call Off Schedule 7: Schedule of Processing, Personal Data and Data Subjects of the Call Off Contract:

Description	Details
Identity of the Controller and Processor	The Parties acknowledge that for the purposes of the Data Protection Legislation, the Customer is the Controller and the Contractor is the Processor in accordance with Clause 23.6.1 of the Call Off Terms.
Subject matter of the Processing	This Call Off Contract sets out the Processing arrangements for the handling of Personal Data within the test and trace system.
Duration of the Processing	The duration of the Processing corresponds to the duration of the Services.
Nature and purposes of Processing	<p>The primary purpose of the Processing undertaken within the system is to provide a reliable and robust system to help identify, contain and control coronavirus, reducing the spread of the virus and save lives. It forms a key part of the NHS Test and Trace Service and supports the government's coronavirus recovery strategy.</p> <p>In summary, the Supplier's data processing activities based on the Customer's instructions are:</p> <ul style="list-style-type: none"> ● Collection: <ul style="list-style-type: none"> ● direct data collection from individuals by manual or automated means; and ● data collected (acquired or received) from the Data Controller and third parties other than the individual. ● Creation:



	<ul style="list-style-type: none">• creation of new data by analytics, inference or analysis; and• creation of new data via aggregation, combination or matching.• Transformation:<ul style="list-style-type: none">• manipulation (parsing, formatting or transformation) of data;• updating, for example, to keep data current; and• masking and pseudonymisation to make it more difficult to identify individuals or anonymisation such that individuals cannot be identified.• Use:<ul style="list-style-type: none">• reading data only; and• presenting, accessing, using or copying data.• Sharing with third parties.• Storage of data including backups.• Deletion of data. <p>The following third party will operate as a Sub Processor:</p> <p>OwnBackup Inc</p> <p>400 Kelby St 19th Floor 07024-2938 Fort Lee USA</p>
Type of Personal Data	<p>The following lists the types of Personal Data that will be processed as part of the Services:</p> <ul style="list-style-type: none">• Capabilities and qualifications of the individual:<ul style="list-style-type: none">• education and professional certifications;• profession and employment information; and• professional affiliations.• Identity of the individual:<ul style="list-style-type: none">• government identities;• identification number;• individual;• person name; and• telephony.



	<ul style="list-style-type: none"> Location of the individual: <ul style="list-style-type: none"> appointments, schedules, calendar entries; environment of the individual; and physical location of the individual. <p>The following lists the Special Categories of Personal Data that will be processed as part of the Services:</p> <ul style="list-style-type: none"> Personal Data revealing racial or ethnic origin; and data concerning health.
Categories of Data Subjects	<p>The following lists the categories of Data Subjects whose Personal Data are processed as part of the Services:</p> <ul style="list-style-type: none"> the Customer's employees (including temporary or casual workers, volunteers, assignees, trainees, retirees, pre-hires and applicants); the Customer's affiliates' employees (including temporary or casual workers, volunteers, assignees, trainees, retirees, pre-hires and applicants); the Customer's (potential) customers (if those (potential) customers are individuals); employees of the Customer's (potential) customers; the Customer's business partners (if those business partners are individuals); employees of the Customer's business partners; the Customer's visitors; the Customer's suppliers and sub-contractors (if those suppliers and sub-contractors are individuals); employees of the Customer's suppliers and sub-contractors; and the Customer's agents, consultants and other professional experts (contractors).
Plan for return of the data once the Processing is complete unless requirement under union or member state law to preserve that type of data	The Customer will be able to delete and/or make a copy of the Personal Data until the expiration or termination of the Services. The Supplier will delete all Personal Data at the end of the Services.
Data Protection Officer Contact	The Supplier's privacy contact can be contacted at ChiefPrivacyOffice@ca.ibm.com
Jurisdiction of the Processing	The jurisdiction of the Processing is as follows:



	<ul style="list-style-type: none"> the Supplier – data processing will be in the UK; and Own{backup} - data stored in the UK. Support is performed outside of the UK in the United States and Israel as follows: <ul style="list-style-type: none"> United States – perform service management and application support but do not have access to Personal Data; and Israel - this team does not have direct access to Personal Data as part of business as usual support. This team may initiate access to the Customer's environment when the Customer chooses to escalate a support ticket. These members of the Own{backup} team may then only access the Customer's environment to investigate the cause of the support issue.
Technical and Organisational Measures	To comply with Clause 23.6 of the Call Off Terms, the Supplier, working with the Customer, will implement the following the Technical and Organisation Measures (also referred to as “ TOMs ”): see table below.

Technical and Organisational Measures that will apply to this Call Off Contract:

Technical Organisation Measure Description
Keep approval records of data security & privacy (DS&P) documents and make available for report/audit purpose.
Create and review DS&P documents in a timely manner and review on a periodic basis.
Store and archive project related documentation in secure repository.
Create and maintain project DS&P documents that reflect the requirements of the TOMs documented in the appropriate contractual document.
Assess the impact of contract changes on the Processing of Personal Data and update DS&P documentation as appropriate.
Undertake pre-screening assessments and have project personnel sign NDAs as appropriate.
Enter into written agreements with all Sub Processors to impose on them substantially similar obligations as are set out in the appropriate contractual document, in particular providing sufficient guarantees to implement appropriate technical and organisational measures.
Define and monitor Service Levels for Sub Processors corresponding to the Service Levels agreed with the Customer.
Monitor and document adherence to the TOMs defined in the appropriate contractual document.
Regularly assess project risks related to processing of Personal Data.
Implement a risk management process.
Document and manage project and data processing risks according to the risk management process.
Manage DS&P aspects of the project utilising project management methodology.
Ensure Personal Data is only processed as agreed in the appropriate contractual document.
Ensure availability of appropriate DS&P skills.
Create and maintain an inventory of Personal Data and security related items.



Create and maintain a list of security operating procedures.
Conduct periodic contract specific DS&P training.
Conduct periodic contract specific DS&P training for Sub Processors.
Manage user access to the project technical environment.
Manage access to the log files.
Require password standards meet the Customer's requirements and/or the Supplier's standards as agreed.
Monitor and log read access to Personal Data.
Monitor and log access from locations outside of the geographic region.
Implement disaster recovery and backup capabilities to recover Personal Data.
Separate development & test environments (including the use of Personal Data) from the production environment.
Log and monitor system activities according to the SOW.
Manage access to and through the Supplier's network in a secure manner.
Establish and adhere to the system and application change process.
Implement testing and validation processes to ensure only authorised changes are promoted to production.
Employ the use of encryption, pseudonymization and/or anonymisation of Personal Data in data processing activities where applicable.
Follow privacy by design principles for the new system.
Govern document handling by the Supplier's policies.
Implement the three lines of defence model where activities are performed to address each line of defence as appropriate based on risks by various test and audit functions.
Follow up action plans resulting from security audits, tests and assessments.
Review the Supplier's security policies, processes and instructions periodically and revise as needed.
Implement an incident management process to ensure immediate reporting, impact analysis and effective corrective (and preventive) actions.
Implement an effective emergency plan ensuring adequate involvement of IBM Legal in security incidents.
Implement procedures for threat prevention for minimising the risk of security breaches.
Manage data security and privacy in accordance with the Supplier's corporate policy and organizational instructions covering regulatory requirements for Processors.
Define data security and privacy roles and responsibilities at the corporate level of the Supplier.
Conduct periodic organisational level DS&P training.
Conduct periodic training for the proper handling of confidential data.
Define password handling rules in the Supplier's corporate instructions and conduct annual training to foster employee awareness.
Control access to the Supplier's sites.
Protect and control access to the systems containing Personal Data.
Implement enhanced security controls in place for delivery and loading areas to prevent unauthorized access to the buildings.
Control access to the Supplier's internal systems in accordance with the Supplier's guidelines.
Provide business continuity through physical protection and by having required infrastructure and processes.
Test and verify the Supplier's internal systems before deployment in production.



Implement security controls for workstations that process Personal Data.
Implement controls for mobile computing and communication infrastructure in accordance with the Supplier's security policies.
Securely destroy sensitive information and licensed software prior to reuse or disposal of equipment.
Conduct privacy by design training for the development teams, as required.

Within the scope of the Call Off Contract, the following clauses shall be added as clause 3.2.11 (Representation and Warranties) of the Call Off Terms:

3.2.11 The current understanding of the Parties is that any Deliverables shall not be considered a Medical Device. A future Release which changes this position will be subject to Variation (or Change for the purposes of Call Off Schedule 5).

Within the scope of the Call Off Contract, the following clauses shall be replaced and added to Clause 18.1 (Supplier Personnel) of the Call Off Terms:

18.1.1(b)(ii) are vetted on a case by case basis dependant on which roles require specific government National Security Vetting clearances (such as 'SC') including system administrators with privileged access to IT systems which store or process Customer Data.

18.1.4 Supplier Personnel are subject to pre-employment checks that include, as a minimum: verification of identity, employment history, unspent criminal convictions and right to work, as detailed in the HMG Baseline Personnel Security Standard (<https://www.gov.uk/government/publications/government-baseline-personnel-security-standard>), as may be amended or replaced by the Government from time to time.

18.1.5 The Supplier shall prevent Supplier Personnel who have not yet received or are unable to obtain the security clearances required by this clause from accessing systems which store, process, or are used to manage Customer Data, or from accessing Customer premises, except where agreed with the Customer in writing.

18.1.6 All Supplier Personnel that have the ability to access Customer Data or systems holding Customer Data shall undergo regular training on secure information management principles. Unless otherwise agreed with the Customer in writing, this training must be undertaken annually.

18.1.7 Where Supplier Personnel are granted the ability to access Customer Data or systems holding Customer Data, those Supplier Personnel shall be granted only those permissions necessary for them to carry out their duties. When Supplier Personnel no longer need such access or leave the organisation, their access rights shall be revoked within one (1) Working Day.

Within the scope of the Call Off Contract, the following clause shall be added as Clause 19.7 of the Call Off Terms:

19.7 Improving visibility of subcontract opportunities available to SMEs and VCSEs in the supply chain

19.7.1 The Supplier shall:



- (a) subject to clause 19.7.3 advertise on Contracts Finder all subcontract opportunities arising from or in connection with the provision of the Services above a minimum threshold of £25,000 that arise during the Call Off Contract Period;
- (b) within ninety (90) days of awarding a sub-contract to a sub-contractor, update the notice on Contracts Finder with details of the successful sub-contractor;
- (c) monitor the number, type and value of the sub-contract opportunities placed on Contracts Finder advertised and awarded in its supply chain during the Contract Period;
- (d) provide reports on the information at clause 19.7.1(c) to the Customer in the format and frequency as reasonably specified by the Customer; and
- (e) promote Contracts Finder to its suppliers and encourage those organisations to register on Contracts Finder.

19.7.2 Each advert referred to in clause 19.7.1(a) above shall provide a full and detailed description of the sub-contract opportunity with each of the mandatory fields being completed on Contracts Finder by the Supplier.

19.7.3 The obligation at Clause 19.7.1(a) shall only apply in respect of sub-contract opportunities arising after the contract award date.

19.7.4 Notwithstanding clause 19.7.1, the Customer may by giving its prior written approval, agree that a sub-contract opportunity is not required to be advertised on Contracts Finder.

Within the scope of the Call Off Contract, the following clause shall be added as Clause 14A of the Call Off Terms:

14A Management Charges and Information

14.1 In addition to any other management information requirements set out in this Call Off Contract, the Supplier agrees and acknowledges that it shall, upon the Customer's request at no charge, provide timely, full, accurate and complete SME Management Information (MI) Reports to the Customer which incorporate the data described in the MI Reporting Template which is:

- (a) the total contract revenue received directly on a specific contract;
- (b) the total value of sub-contracted revenues under the contract (including revenues for non-SMEs/non-VCSEs); and
- (c) the total value of sub-contracted revenues to SMEs and VCSEs.

14.2 The SME Management Information Reports shall be provided in the correct format as required by the MI Reporting Template and any guidance issued by the Customer from time to time. The Supplier shall use the initial MI Reporting Template which is set out below and which may be changed from time to time (including the data required and/or format) by the Customer by issuing a replacement version. The Customer shall give at least thirty (30) days' notice in writing of any such change and shall specify the date from which it must be used.



14.3 The Supplier further agrees and acknowledges that it may not make any amendment to the current MI Reporting Template without the prior written approval of the Customer.



MI Reporting
Template(104342610)

Clause 22.1 A is added to the Call Off Terms to confirm assignment of Project Specific IPR and Specially Written Software to the Customer. For clarity, the entirety of Clause 22 is shown below, to reflect new Clause 22.1 A and consequential changes to other parts of Clause 22, and the version of Clause 22 below shall replace the current version of Clause 22 of the Call Off Terms:

22 Intellectual Property Rights

22.1 A Assignment of Project Specific IPR and Specially Written Software

22.1 A (i) The Customer shall own all rights, title and interest in the Project Specific IPR and Specially Written Software which are delivered to or provided to the Customer in fulfilment of the Supplier's obligations under this Call Off Contract, to the extent that such rights, title and interest are created or come into existence as part of the Services. The Supplier hereby assigns to the Customer with full title guarantee, title to and all rights and interest in the Project Specific IPRs and Specially Written Software (or shall procure that the owner of the Project Specific IPRs and Specially Written Software assigns to the Customer with full title guarantee, title to and all rights and interest in the same) on the same basis. Notwithstanding the above, (a) any rights, title or interest in any Know-How, trade secrets or other rights in Confidential Information relating to information technology including software functionality, which are created solely by the Supplier as part of the Services; and (b) any rights, title or interest in any patents or trade marks, which are created solely by the Supplier as part of the Services, are not assigned to the Customer via this Call Off Contract and shall be owned by the Supplier, unless agreed otherwise in a Variation (and in the event that any such Supplier created intellectual property arises, the Supplier will disclose the same to the Customer and discuss such a Variation with the Customer in good faith acting reasonably). The Customer is hereby granted perpetual, worldwide, royalty-free permission to perform (and authorise Approved Sub-Licensees to perform) any activities which would otherwise infringe any such patents, trade marks, Know-How, trade secrets, or other rights in Confidential Information, which are owned by the Supplier, in the Customer's business or function, both internally and with external parties. This license also extends to any Project Specific IPRs or Specially Written Software which are not delivered or provided to the Customer, but which are nevertheless created in the fulfilment of the Supplier's obligations under this Call Off Contract or come into existence as part of the Services, provided that this license extension shall not result in the relevant rights being assigned to the Customer under the first sentence above, where any relevant materials or other items are delivered or provided to the Customer by the Supplier purely as part of satisfying its obligations under this license extension.

22.1 A (ii) The assignment under Clause 22.1 A (i) shall be a present assignment of future rights that will take effect immediately on the coming into existence of the relevant Project Specific IPRs and/or Specially Written Software, as appropriate.



22.1 A (iii) The Supplier shall waive or procure a waiver of any moral rights in any copyright works assigned to the Customer under this Call Off Contract.

22.1 A (iv) If requested to do so by the Customer, the Supplier shall without charge to the Customer execute all documents and do all such further acts as the Customer may require to perfect the assignment under Clause 22.1 A (i) or shall procure that the owner of the Project Specific IPRs and Specially Written Software does so on the same basis.

22.1 A (v) The Supplier will not include or embed any Supplier Software or other Supplier materials, Third Party Software or Open Source Software, or other third party materials protected by Third Party IPR, in any Project Specific IPRs and Specially Written Software without the Customer's Approval.

22.1 B Allocation of title to IPR

22.1 B1 Save as expressly granted elsewhere under this Call Off Contract:

(a) the Customer shall not acquire any rights, title or interest in or to the Intellectual Property Rights of the Supplier or its licensors, including in the Supplier Software or the Supplier Background IPR, Third Party Software or Third Party IPR; and

(b) the Supplier shall not acquire any rights, title or interest in or to the Intellectual Property Rights of the Customer, including in the Project Specific IPR and Specially Written Software, Customer Software, Customer Background IPR and Customer Data.

22.1 B2 Where either party acquires, by operation of Law, title to Intellectual Property Rights that is inconsistent with the allocation of title set out in this Clause 22.1 B, it shall assign in writing such Intellectual Property Rights as it has acquired to the other Party on the request of the other Party (whenever made).

22.1 B3 Neither Party shall have any right to use any of the other Party's names, logos or trade marks on any of its products or services without the other Party's prior written consent.

22.2 Licences granted by the Customer to the Project Specific IPR and Specially Written Software

22.2.1 Customer hereby grants to the Supplier a royalty-free, non-exclusive, non-transferable licence during the Call Off Contract Period, revocable for breach of its terms, to use the Project Specific IPR and the Specially Written Software, Customer Software, the Customer Background IPR and the Customer Data solely to the extent necessary for providing the Services in accordance with this Call Off Contract, including (but not limited to) the right to grant sub-licences to Sub-Contractors provided that:

(a) any relevant Sub-Contractor has entered into a confidentiality undertaking with the Supplier on the same terms as set out in Clause 23.3 (Confidentiality); and

(b) the Supplier shall not without Approval use the licensed materials for any other purpose or for the benefit of any person other than the Customer.

22.2.2 The Supplier shall not sub-license the rights granted to it pursuant to Clause 22.2 without the Customer's prior written consent.



22.2.3 In the event the Customer consents to a sub-license in accordance with Clause 22.2.2 above, the Supplier must ensure:

- (a) the sub-license is on terms no broader than those granted to the Supplier; and
- (b) the sub-license only authorises the third party to use the rights licensed in Clause 22.2 for the sole purpose of providing the Services.

22.2.4 Customer hereby grants the Supplier (and its affiliated entities) the right to create (and to externally distribute copies of) any materials created by the Supplier in good faith which are substantially similar to any materials for which the copyright is assigned to the Customer via clause 22.1A, provided that all copies of such assigned materials are deleted by the Supplier prior to any work being undertaken which leads to creation of such new materials, and such assigned materials are not used, accessed or referred to in any way and, for the avoidance of doubt, the Supplier is not allowed to use or disclose any Confidential Information that was disclosed to the Supplier by the Customer, in the creation/distribution of such new material.

22.3 Licences granted by the Supplier

22.3.1 The Supplier hereby grants to the Customer a perpetual, royalty-free and non-exclusive licence to use:

- a) the Supplier Software or other materials of the Supplier which the Supplier delivers to the Customer in fulfilment of Supplier's obligations under this Call-Off Contract, or which are included or embedded in any of the Project Specific IPRs and Specially Written Software for any purpose relating to the Services and/or (where applicable) to obtain the full benefits of ownership of the Project Specific IPRs and Specially Written Software, such use including but not limited to the right to load, execute, store, transmit, display and copy (for the purposes of archiving, backing-up, loading, execution, storage, transmission or display) and (in the case of the Project Specific IPRs and Specially Written Software) to modify and exploit the same).
- b) Notwithstanding a), where the Supplier normally licenses such Supplier Software or other materials of the Supplier on standard terms, such standard terms shall apply, instead of the license in this clause 22.3.1 a) , and this shall be agreed by Variation. Such Supplier Software and other materials of the Supplier, and such standard terms, shall be clearly identified in section C of the Order Form.

22.3.2 At any time during the Call Off Contract Period or following the Call Off Expiry Date, the Supplier may terminate a licence granted in respect of the Supplier Software or other materials of the Supplier under Clause 22.3.1 by giving 30 days' notice in writing (or such other period as agreed by the Parties) if there is a Customer Cause which constitutes a material breach of the terms of Clauses 22.3.1(a) or 22.3.1(b) (as the case may be) which, if the breach is capable of remedy, is not remedied within 20 Working Days after the Supplier gives the Customer written notice specifying the breach and requiring its remedy.

22.3.3 In the event the licence of the Supplier Software or other materials of the Supplier is terminated pursuant to Clause 22.3.2, the Customer shall:

- a) immediately cease all use of the Supplier Software or other materials of the Supplier;
- b) at the discretion of the Supplier, return or destroy documents and other tangible materials that contain any of the Supplier Software or other materials of the Supplier, provided that if the Supplier



has not made an election within six (6) months of the termination of the licence, the Customer may destroy the documents and other tangible materials that contain any of the Supplier Software and/or other materials of the Supplier (as the case maybe); and

c) ensure, so far as reasonably practicable, that any Supplier Software or other materials of the Supplier that are held in electronic, digital or other machine-readable form cease to be readily accessible (other than by the information technology staff of the Customer) from any computer, word processor, voicemail system or any other device containing such Supplier Software or other materials of the Supplier

22.4 Customer's right to sub-license

22.4.1 The Customer may sub-license the rights granted under Clause 22.3 to a third party (including for the avoidance of doubt, any Replacement Supplier) provided that:

(a) the sub-licence is on terms no broader than those granted to the Customer; and

(b) the sub-licence only authorises the third party to use the rights licensed in Clause 22.3 for purposes relating to the Services (or substantially equivalent services) or for any purpose relating to the exercise of the Customer's (or, if the Customer is a Central Government Body, any other Central Government Body's) business or function.

22.4.2 The Customer may sub-license the rights granted under Clause 22.3 to any Approved Sub-Licensee to the extent necessary to use and/or obtain the benefit of the Supplier Software or other materials of the Supplier provided that the sub-licence is on terms no broader than those granted to the Customer.

22.5 Customer's right to assign / novate licences

22.5.1 The Customer may assign, novate or otherwise transfer its rights and obligations under the licence granted pursuant to Clause 22.3 to:

(a) a Central Government Body; or

(b) to any body (including any private sector body) which performs or carries on any of the functions and/or activities that previously had been performed and/or carried on by the Customer.

22.5.2 Where the Customer is a Central Government Body, any change in the legal status of the Customer which means that it ceases to be a Central Government Body shall not affect the validity of any licence granted in Clause 22.3. If the Customer ceases to be a Central Government Body, the successor body to the Customer shall still be entitled to the benefit of the licences granted in Clause 22.3.

22.5.3 If a licence granted in Clause 22.3 is novated under this Clause 22.5 or there is a change of the Customer's status pursuant to Clause 22.5.2 (both such bodies being referred to as the "Transferee"), the rights acquired by the Transferee shall not extend beyond those previously enjoyed by the Customer.

22.6 Third Party Software

22.6.1 The Supplier shall procure that the owners or the authorised licensors of any and any Third Party Software which is not commercial off-the-shelf software grant a direct licence to the



Customer on terms at least equivalent to those set out in Clause 22.3.1 and Clause 22.5. If the Supplier cannot obtain for the Customer a licence materially in accordance with the licence terms set out in Clause 22.3.1 and Clause 22.5 in respect of any such Third Party Software, the Supplier shall:

(a) notify the Customer in writing giving details of what licence terms can be obtained from the relevant third party and whether there are alternative software providers which the Supplier could seek to use; and

(b) only use such Third Party Software if the Customer Approves the terms of the licence from the relevant third party.

22.6.2 The Supplier shall procure that the owners or the authorised licensors of any Third Party Software which is commercial off-the-shelf software grants a direct licence to the Customer on terms no less favourable than such software is usually made available.

22.7 Other licences granted by the Customer

22.7.1 The Customer hereby grants to the Supplier a royalty-free, non-exclusive, non-transferable licence during the Call Off Contract Period to use the Customer Software, the Customer Background IPR and the Customer Data solely to the extent necessary for providing the Services in accordance with this Call Off Contract, including (but not limited to) the right to grant sub-licences to Sub-Contractors provided that:

a) any relevant Sub-Contractor has entered into a confidentiality undertaking with the Supplier on the same terms as set out in Clause 23.3 (Confidentiality); and

b) the Supplier shall not without Approval use the licensed materials for any other purpose or for the benefit of any person other than the Customer.

22.8 Termination of licences

22.8.1 Subject to Clauses 22.3.2 and/or 22.3.3 (Licences granted by the Supplier), all licences granted pursuant to this Clause 22 (Intellectual Property Rights) shall survive the Call Off Expiry Date (other than those granted pursuant to Clause 22.6.2 (Third Party Software) and 22.7.1 (Other Licences granted by the Customer)).

22.8.2 The Supplier shall, if requested by the Customer in accordance with Call Off Schedule A4 (Exit Management) where used, grant (or procure the grant) to the Replacement Supplier of a licence to use any Supplier Software or other materials of the Supplier, and/or Third Party Software on terms equivalent to those set out in Clause 22.3.1 (Licences granted by the Supplier) subject to the Replacement Supplier entering into reasonable confidentiality undertakings with the Supplier.

22.8.3 The licences granted by the Customer to the Supplier pursuant to this Clause 22 and any sub-licence granted by the Supplier in accordance with this Clause 22 shall terminate automatically on the Call Off Expiry Date and the Supplier shall:

a) immediately cease all use of the Project Specific IPR and Specially Written Software assigned to the Customer, Customer Software, the Customer Background IPR and the Customer Data (as the case may be);



b) at the discretion of the Customer, return or destroy documents and other tangible materials that contain any of the Project Specific IPR and Specially Written Software, Customer Software, the Customer Background IPR and the Customer Data, provided that if the Customer has not made an election within six months of the termination of the licence, the Supplier may destroy the documents and other tangible materials that contain any of the Project Specific IPR and Specially Written Software, Customer Software, the Customer Background IPR and the Customer Data (as the case may be); and

c) ensure, so far as reasonably practicable, that any Project Specific IPR and Specially Written Software, Customer Software, Customer Background IPR and Customer Data that are held in electronic, digital or other machine-readable form ceases to be readily accessible from any computer, word processor, voicemail system or any other device of the Supplier containing such Project Specific IPR and Specially Written Software, Customer Software, Customer Background IPR and/or Customer Data.

22.9 IPR Indemnity

22.9.1 The Supplier shall during and after the Call Off Contract Period, on written demand indemnify the Customer against all Losses incurred by, awarded against or agreed to be paid by the Customer (whether before or after the making of the demand pursuant to the indemnity hereunder) arising from an IPR Claim provided that, where reasonably possible, the Customer provides the Supplier with advance notice before incurring any costs or expenses. However, where the subject of the IPR Claim is a patent, the Supplier's payment obligations shall be limited such that the Supplier shall pay only any amounts (including for the avoidance of doubt all damages, costs, and interest) contained in a final court judgement or settlement approved by the Supplier, as well as any reasonable legal fees and other reasonable expenses directly associated with, and paid together with, such legal fees, the Customer incurs up to the time when the Customer notifies the Supplier of the receipt of the IPR Claim.

22.9.2 If an IPR Claim is made, or the Supplier anticipates that an IPR Claim might be made, the Supplier may, at its own expense and sole option, either:

(a) procure for the Customer the right to continue using the relevant item which is subject to the IPR Claim; or

(b) replace or modify the relevant item with non-infringing substitutes provided that:

(i) the performance and functionality of the replaced or modified item is at least equivalent to the performance and functionality of the original item;

(ii) the replaced or modified item does not have an adverse effect on any other Services or the ICT Environment;

(iii) there is no additional cost to the Customer; and

(iv) the terms and conditions of this Call Off Contract shall apply to the replaced or modified Services.

22.9.3 If the Supplier elects to procure a licence in accordance with Clause 22.9.2(a) or to modify or replace an item pursuant to Clause 22.9.2(b), but this has not avoided or resolved the IPR Claim, then:



- (a) the Customer may terminate this Call Off Contract by written notice with immediate effect; and
- (b) without prejudice to the indemnity set out in Clause 22.9.1, the Supplier shall be liable for all reasonable and unavoidable costs of the substitute services including the additional costs of procuring, implementing and maintaining the substitute items.

22.9.4 The provisions of Clauses 22.9.1 to 22.9.3 (inclusive) shall not apply to the extent that any IPR Claim is caused by:

- a) any modifications, made by any party other than the Supplier, to any material which the Supplier delivers to the Customer, unless the Supplier agrees in writing that such party should make the specific modifications which give rise to the claim, as part of the Services;
- b) any material, including any Software, which originates from a third party, unless the Supplier contracts directly with the third party to license any such material (including any Software) and the Customer is not a party to such license contract, and the Customer has no right to use such material (including any Software) at termination;
- c) the Supplier's compliance with any instructions, designs, requirements, content or specifications of the Customer, unless the Supplier's employees who are directly involved in providing the Services have actual knowledge of the relevant IPR of a third party which results in the IPR Claim and have actual knowledge that delivery of the relevant materials would infringe the relevant IPR; and
- d) any use by or on behalf of the Customer of any material which the Supplier has not delivered to the Customer.

22.9.5 As conditions on the Supplier's obligations above the Customer agrees that:

- (a) it will promptly notify the Supplier in writing of any IPR Claim;
- (b) it will allow the Supplier to conduct all negotiations and proceedings and will provide the Supplier with such reasonable assistance required by the Supplier, and will comply with Supplier's reasonable requests, including with respect to mitigation efforts, each at the Supplier's cost, regarding the IPR Claim; and
- (c) it will not, without first consulting with the Supplier, agree to make any payment or make an admission relating to the IPR Claim.

22.9.6 The Supplier shall consider and defend the IPR Claim diligently using competent counsel and in such a way as not to bring the reputation of the Customer into disrepute. The Supplier shall not settle or compromise any IPR Claim without the Customer's Approval (not to be unreasonably withheld or delayed) except that the Customer's Approval shall be deemed given where the settlement or compromise involves no obligations on the part of the Customer, such as where the settlement involves only the payment of a monetary amount in exchange for the right to continued use of the relevant delivered material.

22.9.7. For the purposes of this section 22.9, the definition of IPR Claim shall be as follows:

"IPR Claim" means any claim of infringement or alleged infringement of any IPR owned by a third party by any software or other materials which the Supplier delivers to the Customer in fulfilment of Supplier's obligations under this Call Off Contract. For the avoidance of doubt, an IPR Claim



shall include a claim that is received by a party performing services for the Customer, who uses, on behalf of the Customer, materials which the Supplier delivers to the Customer in fulfilment of Supplier's obligations under this Call Off Contract, where such claim is referred or notified, by such party, to the Customer for handling such claim and/or pursuant to an indemnity given by the Customer in respect of such claim and, where the Customer is responsible to such party for handling, providing an indemnity in respect of or otherwise liable to such party for such claim.

22.9.8. Nothing in this section 22.9 shall exclude or restrict the Customer's general obligation at law to mitigate any Losses which are covered under this indemnity. The obligations of the Supplier as stated in this section 22.9 are the Customer's exclusive remedy for any IPR Claim.

22.10 Open Source Software

22.10.1 If the Supplier wishes to use Open Source Software (which is, computer software that has its source code made available subject to an open source licence under which the owner of the copyright and other IPRs in such software provides the rights to use, study, change and distribute the software to any and all persons and for any and all purposes free of charge) then the Supplier shall:

- a) notify the Customer in writing giving details of the licence terms and whether there are alternative software providers which the Supplier could seek to use;
- b) identify all items of Open Source Software used and proposed to be used in an up to date register of Open Source Software; and
- c) provide copies of the Open Source Software register and the licences upon request by the Customer.

Within the scope of the Call Off Contract, the following clauses shall be added to Clause 23.6 (Data Protection) of the Call Off Terms:

23.6.4.4.5 in respect of any processing in, or transfer of Personal Data to, any Restricted Country permitted in accordance with this Clause 23.6.4.4, the Supplier shall, when requested by the Customer, promptly enter into an agreement with the Customer or any service recipient including or on such provisions as the Standard Contractual Clauses and/or such variation as a regulator or the Customer might require which terms shall, in the event of any conflict, take precedence over those in this Clause 23.6, and the Supplier shall comply with any reasonable instructions notified to it in advance by the Customer with respect to the transfer of the Personal Data;

23.6.15 Both the Customer and the Supplier shall comply with their respective obligations under the GDPR that arise in relation to the Processing activities that the Customer instructs the Supplier to perform under this Call Off Contract, including by adhering to any relevant codes of conduct published pursuant to Article 40 of the GDPR, for which the Customer as Data Controller will notify the Supplier as Data Processor as part of the Processing instructions and shall provide the Supplier with the opportunity to object to instructions for justified reasons. Any such relevant codes of conduct published pursuant to Article 40 that have an impact on the Services may be subject to Variation (or Change for the purposes of Call-Off Schedule 5).

23.6.16 If following the date of this Call Off Contract:



23.6.16.1 any codes of practice, codes of conduct, regulatory guidance, standard clauses and any other related laws arising from the GDPR are published; or

23.6.16.2 the UK ceases to be a Member State of the European Union, then the Customer may require the Supplier to take such further reasonable actions, or enter into such further contractual terms, in each case as necessary to take account of these developments subject to Variation (or Change for the purposes of Call-Off Schedule 5).

23.6.17 Subject to clauses 25.2.1(c), 25.3.1 and 25.5.1, the Supplier shall at all times during and after the expiry of the Call Off Contract, indemnify the Customer and keep the Customer indemnified against all losses, damages, costs or expenses and other liabilities (including legal fees) incurred by, awarded against or agreed to be paid by the Customer arising from any breach of the Supplier's obligations under this clause 23.6.

Within the scope of the Call Off Contract, the following clause shall be added as Clause 23.6A of the Call Off Terms:

23.6A The Supplier shall, at its own cost, participate and provide full co-operation for the completion of any Data Protection Impact Assessments conducted by the Customer relating to the Services, such participation and co-operation shall include updating the Data Protection Impact Assessment upon each Release and following any Variation (or Change for the purposes of Call Off Schedule 3).

Within the scope of the Call Off Contract, Clause 23.6.4.4 shall be amended and replaced with the following:

23.6.4.4 not transfer Personal Data outside of the United Kingdom unless the prior written consent of the Customer has been obtained and the following conditions are fulfilled:

For clarity, the remaining text set out in the current version of Clause 23.6.4.4 of the Call-Off Terms shall remain as drafted and shall not be deleted, amended or replaced other than as set out in this Order Form.

Within the scope of the Call Off Contract, Clause 25.2.1(b) shall be deleted in its entirety and replaced with the following Clause 25.2.1(b):





Within the scope of the Call Off Contract, the following clause shall be added as Clause 13A of the Call Off Terms:

13A Governance

The Supplier shall provide a proposed process for governance arrangements (which shall include details of any meetings to be attended by both Customer and Supplier Personnel) within twenty (20) days of signature of the Order Form. The proposed governance arrangements shall be subject to the Customer's Approval in accordance with Clause 5.5 of the Call Off Terms.

Within the scope of the Call Off Contract, the following clause shall be added as Clause 13B of the Call Off Terms:

13B Responsibility Matrix

The Supplier shall provide a responsibility matrix which shall include details of Customer and Supplier responsibilities relating to the Services within twenty (20) days of signature of the Order Form. The responsibility matrix shall be subject to the Customer's Approval in accordance with Clause 5.5 of the Call Off Terms.

Within the scope of the Call Off Contract, the following clause shall be added as Clause 5.5 of the Call Off Terms:

5.5 Deliverables Acceptance Process

5.5.1 Within five (5) Working Days of the submission of any Deliverables, or other reasonable period as agreed by the Parties, the Customer shall review and either accept, or provide a single set of consolidated comments on the Deliverable.

5.5.2. Where comments are provided by the Customer, the Supplier will have three (3) Working Days from its receipt thereof, or such other reasonable period as agreed by the Parties, to update the Deliverable to address the comments.

5.5.3. The Supplier shall resubmit the revised Deliverable to the Customer within such three (3) Working Day period, or such other reasonable period as agreed by the Parties, for review, in accordance with the preceding provisions of this Clause.

5.5.4 In the event that the Deliverable has not been agreed by both Parties on completion of two review cycles, the Parties shall meet promptly to resolve the outstanding issues prior to acceptance.

5.5.5. Non-Approval is to be managed via Dispute Resolution Procedure set out in Schedule 4 of the Call Off Contract.

5.5.6 The Supplier shall in no event be penalised for non-timely Customer Approval of Deliverables and will escalate through the governance process where this could cause knock on impacts to the delivery of the Services and/or Achievement of a Milestone by the Milestone Date.

Within the scope of the Call Off Contract, the following paragraph shall be added as Paragraph 5A of Schedule 2 (Call Off Contract Charges, Payment and Invoicing) of the Call Off Terms:



5A Electronic Invoicing

5A.1 The Customer shall accept and process for payment an electronic invoice submitted for payment by the Supplier where the invoice is undisputed and where it complies with the standard on electronic invoicing.

5A.2 For the purposes of paragraph 5A.1, an electronic invoice complies with the standard on electronic invoicing where it complies with the European standard and any of the syntaxes published in Commission Implementing Decision (EU) 2017/1870.

Within the scope of the Call Off Contract, the following clauses shall be added to the Call Off Terms:

16.6 IR35

16.6.1 This Call Off Contract constitutes a contract for the provision of goods and/or services. Where the Supplier (or its Sub-Contractors) have included one or more people that are non-permanent members of staff that are not on the Supplier's (or its Sub-Contractors) payroll ("**Contractor(s)**") to fulfil its service obligations under this Call Off Contract, the Supplier shall be fully responsible for and shall indemnify the Customer for:

- (a) any proceedings, claims or demands by any third party (including specifically, but without limitation, HMRC and any successor, equivalent or related body pursuant to the IR35 legislation and/or any of the provisions of Income Tax Regulations);
- (b) any income tax, National Insurance and social security contributions and any other liability, deduction, contribution, assessment or claim arising from or made in connection with either the performance of the services or any payment or benefit received by the Contractor in respect of the services, where such recovery is not prohibited by law; and
- (c) all reasonable costs, expenses and any penalty, fine or interest incurred or payable by the Customer in connection with or in consequence of any such liability, deduction, contribution, assessment or claim.

16.6.2 The Customer may at its option satisfy such indemnity (in whole or in part) by way of deduction from payments due to the Supplier.

16.6.3 The Supplier warrants that it is not, nor will it prior to the cessation of this Call Off Contract, become a managed service company, within the meaning of section 61B of the Income Tax (Earnings and Pensions) Act 2003.

16.6.4 The Supplier shall monitor the provision of the services and notify the Customer where it considers that the activity of the Customer may impact the Suppliers' (or its Sub-Contractors) IR35 assessment in relation to the Contractors.

23.6A. Cyber Security Requirements

The Supplier warrants and represents that it has complied with and throughout the Call Off Contract Period will continue to comply with the Cyber Security Requirements.



35.5 Corporate Social Responsibility Conduct and Compliance

35.5.1 The Customer applies corporate and social responsibility values to its business operations and activities which are consistent with the Government's corporate social responsibility policies, including, without limitation, those policies relating to anti-bribery and corruption, health and safety, the environment and sustainable development, equality and diversity.

35.5.2 The Supplier represents and warrants that it:

- (a) complies with all CSR Laws;
- (b) requires its Sub-Contractors and any person under its control, to comply with all CSR Laws; and
- (c) has adopted a written corporate and social responsibility policy that sets out its values for relevant activity and behaviour (including, without limitation, addressing the impact on employees, clients, stakeholders, communities and the environment by the Supplier's business activities).

35.5.3 The Supplier shall notify the Customer in the event that its corporate and social responsibility policies conflict with, or do not cover the same subject matter in an equivalent level of detail as is in, the CSR Policies.

35.6 Modern Slavery

35.6.1 The Supplier represents and warrants that at the Call Off Commencement Date neither the Supplier, nor any of its officers, employees:

- (a) have been convicted of any offence involving slavery and human trafficking; and
- (b) having made reasonable enquiries, so far as it is aware, have been or is the subject of any investigation, inquiry or enforcement proceedings by any governmental, administrative or regulatory body regarding any offence or alleged offence of or in connection with slavery and human trafficking.

35.6.2 The Supplier shall implement due diligence procedures for its Sub-Contractors and other participants in its supply chains to ensure that there is no slavery or human trafficking in its supply chains.

35.6.3 The Supplier shall prepare and deliver to the Customer each year, an annual slavery and human trafficking report setting out the steps it has taken to ensure that slavery and human trafficking is not taking place in any of its supply chains or in any part of its business.

36.2.A. Assignment and Novation

The Customer may at its discretion assign, novate or otherwise dispose of any or all of its rights, obligations and liabilities under this Call Off Contract and/or any associated licences to the Department of Health and Social Care, the National Institute for Health Protection, NHS England and / or any Central Government Body and the Supplier shall, at the Customer's request, enter into a novation agreement in such form as the Customer shall reasonably specify in order to enable the Customer to exercise its rights pursuant to this Clause 36 (Assignment and Novation).



47. EXECUTION AND COUNTERPARTS

47.1 This Call Off Contract may be executed in any number of counterparts (including by electronic transmission), each of which when executed shall constitute an original but all counterparts together shall constitute one and the same instrument.

47.2 Execution of this Call Off Contract may be carried out in accordance with the Electronic Identification and Trust Services for Electronic Transactions Regulations 2016 (SI 2016/696) and the Electronic Communications Act 2000. In the event each Party agrees to sign this Call Off Contract by electronic signature (whatever form the electronic signature takes) it is confirmed that this method of signature is as conclusive of each Party's intention to be bound by this Call Off Contract as if signed by each Party's manuscript signature. In such situation, this Call Off Contract shall be formed on the date on which both Parties have electronically signed the Call Off Contract as recorded in the Customer's electronic contract management system.

For the purposes of incorporation of Schedule 1 (Definitions) of the Call Off Terms, the following definitions shall be added (and where such terms are already defined, such definitions shall be replaced with the corresponding definitions below):

"Change" for the purpose of Call Off Schedule 3 (Service Levels, Service Points and Performance Monitoring) only, means any planned activity that involves the addition, modification or removal of anything that could have an effect on the Services. The scope of these activities includes, but is not limited to, changes to architecture, processes, tools, IT services or their components;

"Change Advisory Board" or "CAB" means the collective group of customers' stakeholders who review and collectively approve all Supplier Requests For Change;

"Contracts Finder" means the Government's publishing portal for public sector procurement opportunities;

"CSR Laws" means Laws relating to corporate social responsibility issues (e.g. anti-bribery and corruption, health and safety, the environmental and sustainable development, equality and diversity), including but not limited to the Modern Slavery Act 2015, the Public Services (Social Value) Act 2012, the Public Contracts Regulations 2015 and Article 6 of the Energy Efficiency Directive 2012/27/EU, from time to time in force;

"CSR Policies" means the Customer's policies, including, without limitation, anti-bribery and corruption, health and safety, the environmental and sustainable development, equality and diversity, and any similar policy notified to the Supplier by the Customer from time to time, and **"CSR Policy"** shall mean any one of them;

"Customer Level 1" means support for basic Customer issues such as solving usage problems, password re-sets, and fulfilling Service Requests that require IT involvement;

"Customer Service Bridge" means a 24 x 7 x 365 specialist group that provides HSSI governance and management with on-ward communication routes for Customer service stakeholders;

"Cyber Security Requirements" means:

a) compliance with the DSP Toolkit or any replacement of the same; and



b) any other cyber security requirements relating to the Services notified to the Supplier by the Customer from time to time;

“DSP Toolkit” means the data security and protection toolkit, an online self-assessment tool that allows organisations to measure their performance against the National Data Guardian’s 10 data security standards and supports key requirements of the GDPR, which can be accessed from <https://www.dsptoolkit.nhs.uk/>, as may be amended or replaced by the Customer or the Department of Health and Social Care from time to time;

“Emergency CAB” means an ad hoc Change Advisory Board scheduled specifically for the purpose of reviewing and approving an Emergency Change;

“Emergency Change” for the purposes of Call Off Schedule 3 (Service Levels, Service Points and Performance Monitoring) only, means a change that needs to be implemented to prevent the occurrence of a Severity 1 or Severity 2 Incident or which needs to be implemented to Resolve a Severity 1 or Severity 2 Incident;

“End User” means an individual who uses the Service;

“Force Majeure” or “Force Majeure Event” means any event, occurrence, circumstance, matter or cause affecting the performance by either the Customer or the Supplier of its obligations arising from:

a) acts, events, omissions, happenings or non-happenings beyond the reasonable control of the Affected Party which prevent or materially delay the Affected Party from performing its obligations under this Call Off Contract;

b) riots, civil commotion, war or armed conflict, acts of terrorism, nuclear, biological or chemical warfare;

c) acts of the Crown, local government or Regulatory Bodies;

d) fire, flood or any disaster; and

e) an industrial dispute affecting a third party for which a substitute third party is not reasonably available but excluding:

i) any industrial dispute relating to the Supplier, the Supplier Personnel (including any subsets of them) or any other failure in the Supplier or the Sub-Contractor’s supply chain; and

ii) any event, occurrence, circumstance, matter or cause which is attributable to the wilful act, neglect or failure to take reasonable precautions against it by the Party concerned; and

iii) any failure of delay caused by a lack of funds;

However, any event or other consequence arising as a result of biological viruses or infectious diseases with an impact materially similar to COVID 19 or the COVID 19 virus will not constitute a Force Majeure Event;



“General Change in Law” means a change in Law which comes into force after the Call Off Commencement Date, where the change is of a general legislative nature and/or affects or relates to a Comparable Supply, and includes Laws arising out of or in connection with the United Kingdom's withdrawal from the European Union which substantially amend, replace or supersede any existing Law;

“Go Live” means assumption by the Supplier of Operational Responsibility for the performance of the MVP Supplier Operational Support following the Release of the solution into production;

“High Severity Service Incident” or **“HSSI”** means either a Severity 1 or Severity 2 Incident;

“Incident” means an unplanned incident or interruption to Services, reduction in the quality of the Services or event which could affect the Services in the future;

“Incident Record” means the record of the details and history of an Incident created by the Supplier on the Service Management Toolset, in accordance with the incident management process set out in Part C: Service Management below;

“Incident Resolution” means the process by which an Incident is Resolved;

“Known Error” means a fault, identified through investigations into the Root Cause of a Problem, for which a Permanent Fix has been identified but not implemented;

“Level 2” means support provided by the Supplier who has detailed knowledge of the Service and can triage incidents and perform routine fixes;

“Level 3” means support provided by the Supplier who has in-depth knowledge of the application and can triage incidents and perform complex fixes;

“Linked Incident” means an Incident that has been associated with a Master Incident;

“Linked Incident Record” means an Incident Record for Linked Incidents;

“Medical Device” means any Deliverable that falls under the definition of a medical device in accordance with guidance published by the Medicines and Healthcare Products Regulatory Agency;

“Logged” means:

- (a) in relation to a Problem, details of the Problem have been logged on the Service Management Toolset and a Problem Record has been created; and
- (b) in relation to an Incident, details of the Incident have been logged on the Service Management Tool and an Incident Record has been created.

“Log” and **“Logging”** shall be construed according;

“Maintenance” means a collection of one or more changes that have been tested together and will be deployed together to resolve one or more Incidents and / or Problems. A Maintenance Release does not include the introduction of new functionality;



"Master Incident" means the first instance of an Incident being Logged for any related occurrences that are not part of the standard operation of the Services which causes, or may cause, an interruption to or a reduction in the quality of the Services;

"Master Incident Record" means an Incident Record for Master Incidents;

"MVP" is the minimum viable product as defined by the Customer's requirements in the ITT MVP Requirements Catalogue in Section D and then accepted on completion of Statement of Work - MVP – Trace Minimum Viable Product (MVP);

"MVP Supplier Operational Support" is set out in Section D Statement of Work, (MVP Supplier Operational Support);

"Operational Responsibility" means the provision of the Supplier Service Desk in support of the MVP solution in production in accordance with the Service Levels;

"Permanent Fix" means a fix that resolves the underlying Root Cause of a Problem;

"Problem" means, in respect of one or more existing or potential Incidents, either:

- (a) the unknown Root Cause, or
- (b) a known Root Cause that has yet to be Resolved;

"Problem Record" means a record of the details and history of a Problem raised by the Supplier on the Service Management Toolset in accordance with the problem management process set out in Part C: Service Management below;

"PIM" means Process Interface Manual, a document to describe the interlock and integration of the service operations;

"Product Owner" means the Customer representative to the delivery team providing feedback to and sign-off of required deliverables. In addition to this, a key activity is to manage and make visible the product backlog, or the prioritized list of requirements for future product development;

"Release" means an item produced primarily to extend, alter or improve the Software and/or any Deliverable by providing additional functionality or performance enhancement (whether or not defects in the Software and/or Deliverable are also corrected) while still retaining the original designated purpose of that item;

"Release and Maintenance Plan" means a schedule that contains details of the Releases and Maintenance activity;

"Request for Change" or "RFC" means the form that is submitted to the Change Advisory Board by either the Customer or the Supplier detailing any request for change;

"Resolution" means an action taken by or on behalf of the Supplier to fully repair the root cause of an Incident or to implement a workaround and confirmed to the reasonable satisfaction of the Customer. For the avoidance of doubt, the End User shall be able to access and utilise all functions



of the Services again without degradation for an Incident or workaround to be a Resolution. **"Resolve"** and **"Resolved"** shall be construed accordingly;

"Resolution Time" means:

- (a) in relation to an Incident, the length of time it takes the Supplier to Resolve the Incident; or
- (b) in relation to a Problem, the length of time it takes the Supplier to successfully implement a Permanent Fix for the Problem;

"Restricted Country" means any country which is not (i) a member of the European Economic Area; (ii) the United Kingdom; (iii) deemed adequate by the European Commission pursuant to article 25(6) of Directive 95/46/EC or article 45(3) of the General Data Protection Regulation;

"Root Cause" means the underlying reason for the occurrence of an Incident, Defect or Problem (as the case may be);

"Service Bridge" means the Customer's function responsible for the management and communication of HSSIs;

"Service Desk" or **"Help Desk"** means the single point of contact Service Desk set up and operated by the Customer;

"Supplier Service Desk" means the single point of contact service desk operated by the Supplier to receive incidents from the Service Desk;

"Service Request" means a request from an End User, service recipient or the Customer for information, or advice, or for a standard activity provided by the Service Desk. For example to reset a password or to unlock an account;

"Service Management Toolset" or **"Incident Management Tool"** means a toolset which shall at its core act as a workflow management system for handling Incidents, Service Requests, Problems and Changes. This shall also include a tool for configuration management and the ability to enable easy linking between Incidents, Service Request, Problems and Change records with each other and with records of configuration items. The Service Management Toolset shall align to ITIL standards;

"Severity Level" means the level of severity allocated to an Incident or a Problem by the Supplier (or the Customer as applicable);

"SME" means an enterprise falling within the category of micro, small and medium-sized enterprises defined by the Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises;

"Standard Contractual Clauses" means the standard contractual clauses for the transfer of Personal Data to Processors established in third countries which do not ensure an adequate level of protection as set out in Commission Decision C (2010) 593 and reference to the standard contractual clauses shall be to the clauses as updated, amended, replaced or superseded from time to time by the European Commission;

"Support Communication" means any written communication sent from the Supplier to the Customer or other stakeholders relating to an Incident or a Problem; and

"VCSE" means a non-governmental organisation that is value-driven and which principally reinvests its surpluses to further social, environment or cultural objectives.



Within the scope of the Call Off Contract, the following paragraphs shall be added as Part C of Schedule 3 (Service Levels, Service Credits and Performance Monitoring) of the Call Off Terms:

Part C: Service Management

1. Service Desk

1.1 The Supplier Service Desk shall provide the following functions and be the single point of contact that allows the Customer's Service Desk to:

- 1.1.1 receive notification of Incidents and Service Requests via telephone and electronic means (including email and other web based systems);
- 1.1.2 request and receive updates on the progress and/or Resolution of specific Incidents, Problems and Service Requests via telephone or other electronic means; and
- 1.1.3 escalate or complain about the standard of any service provided by the Supplier and logging of Incidents from the Customer's Service Desk.

1.2 The Supplier Service Desk shall, for the duration of the Call Off Contract, record all contacts received by telephone and email on an appropriate Service Management Toolset and provide each caller with a unique Incident reference number for that contact. Any contacts in relation to an existing Incident would be recorded against the existing Incident reference.

1.3 The Supplier will confirm the Severity Level allocated to each Incident or Service Request however the Customer will retain the right to set the Severity Level as deemed appropriate.

1.4 If the Supplier disagrees with any reallocation of the Severity Level by the Customer, then the Supplier shall be entitled to raise the issue at the Performance Review Meeting. Failing agreement, the issue shall be dealt with in accordance with the Dispute Resolution Procedure.

1.5 The Supplier shall provide supporting information as may reasonably be required and / or requested by the Customer or in order to verify that all contacts have been recorded.

1.6 The Supplier's Service Desk shall be responsible for the Incident escalation and complaints process.

1.7 The Supplier will be required to produce a Monthly extract of all Incidents and Service Requests received within the Month.

1.8 The Service Desk shall at all times reasonably co-operate with other service desks associated with the provision of services to the Customer, the Customer's other suppliers and/or any service recipient in the investigation and resolution of Incidents associated with the Services.



- 1.9 The Supplier shall ensure that the Supplier Service Desk is available during the defined Core Hours.
- 1.10 The Supplier shall ensure that the Supplier Service Desk call number is either free or chargeable at local rates. Premium rate numbers are not permissible.
- 1.11 The Supplier shall ensure that the Supplier Service Desk complies with the requirements of the Equality Act 2010, specifically in regard to disability.
- 1.12 The Supplier Service Desk shall not alter any identifiable Personal Data on any systems provided under this Call Off Contract, and the Supplier must ensure that the capture, retention and management of any Personal Data complies with Data Protection Legislation and Customer standards on the protection of Personal Data, including processing of third party data.

2. Incident Management

Creating and maintaining Incident Records

- 2.1 The Supplier shall raise an Incident Record on the Incident Management Tool as soon as the Supplier:
- (a) becomes aware of an Incident in; or
 - (b) is requested to raise an Incident Record by the Customer (acting reasonably), where an Incident Record should have already been raised under the provisions of this Call Off Schedule.
- 2.1.2 The Supplier must create an Incident Record for every Master Incident and every Linked Incident that it becomes aware of.
- 2.1.3 The Supplier shall be deemed to have become aware of an Incident (Master or Linked) on the earlier of:
- (a) when the relevant Incident is reported to the Supplier's Service Desk (including reports received directly in to the Incident Management Tool from another supplier via an automated process);
 - (b) when the Supplier receives an email or other electronic notification (including web logging facilities) regarding the relevant Incident;
 - (c) (for Master Incidents only) when the Supplier identifies (or where it should have identified through its normal operational activities) the relevant Incident itself, via its own Performance Monitoring System or otherwise. For the purposes of this paragraph, normal operational activities shall be deemed to include any obligations that the Supplier is required to fulfil pursuant to or in connection with this Call Off Contract.
- 2.1.4 Where the Supplier is notified about several Incidents via a contact, the Supplier shall create a separate Incident Record for each Incident.



2.1.5 The Supplier is responsible for logging Incidents identified by both reactive and proactive Incident management methods (through the use of Performance Monitoring), including those reasonably requested by the Customer from time to time

2.1.6 In relation to each Incident, the Supplier is responsible for:

- (a) allocating the Incident with a Severity Level using the guidance set out in the Order Form ("**Severity Level Guidelines**");
- (b) continuously monitoring and updating the Severity Level of an Incident as required, in accordance with the Severity Level Guidelines;
- (c) allocating the Incident as a Master Incident or a Linked Incident;
- (d) assessing which Services are affected by the Incident (and updating this throughout the lifecycle of the Incident);
- (e) recording on each Incident Record (Master or Linked), during the lifecycle of the Incident; and
- (f) the Supplier shall record the reason for any change that is made to an Incident Record on the Incident Management Tool after the Incident has been closed, and provide a report detailing the changes and the reasons for each change to the Customer at the Customer's request.

2.1.7 Upon request, the Supplier shall update the Customer about the expected Resolution Time of an Incident.

2.2 Master and Linked Incidents

2.2.1 The Supplier shall employ a Master Incident and Linked Incident hierarchy for Logging and managing Incident Records on its Incident Management tool.

2.2.2 A separate Incident is created (and shall be Logged by the Supplier) in respect of every Incident that the Supplier becomes aware of and every subsequent report of an Incident of the same type made to the Supplier by the Customer or its representative.

2.2.3 Incidents shall be either classified as a Master Incident or a Linked Incident depending on the circumstances as described below.

- (a) A Master Incident is the first (or only) Incident of its type. When a Master Incident exists, any Incident reported to the Supplier by the Customer or its representative which mirrors an existing Master Incident based on the following factors, will be classed as a Linked Incident if:
 - (i) the impact of the Incident is the same or similar to the impact of the Master Incident;
 - (ii) the Incident relates to the same occurrence;



- (iii) initial analysis suggests that the fix necessary to be applied to the Master Incident would be the same as the fix necessary to Resolve the Linked Incident; and
 - (iv) following execution of a Permanent Fix, it is confirmed that the same fix did in fact Resolve all Linked Incidents.
- (b) A Master Incident shall be created as a result of:
- (i) an Incident being reported to the Supplier by the Customer or its representative; or
 - (ii) the Supplier otherwise becoming aware of such an Incident.
- (c) There shall only be one Master Incident (and one Master Incident Record) for each Incident of its type.

2.2.4 Where a Master Incident has been logged, the Supplier shall only Log a Linked Incident following a report of any subsequent Incidents exhibiting the same root cause or user impact.

2.2.5 On any occasion that a Linked Incident is Logged, the Supplier shall automatically create an Incident Record which shall contain identical Incident details to the original Master Incident Record (save that it shall be classified as a Linked Incident and retain its unique identifier). The reason for the creation of an identical Linked Incident Record is to allow all Incidents to be included within the appropriate measurement of the Service Levels.

2.2.6 All Linked Incident Records shall be related to the Master Incident Record within the Incident Management Tool (and vice versa) so that all associated Linked Incidents records can be easily identified and reported against.

2.2.7 A Master Incident may exist without any associated Linked Incidents; however a Linked Incident must be related to an existing Master Incident.

2.2.8 The Supplier shall use all reasonable endeavours to identify associated Incidents prior to the relevant Incidents being Resolved. Once identified, the Supplier must categorise associated Incidents as Master Incidents or Linked Incidents (as applicable) in the Incident Record.

2.2.9 In the event that the Supplier does not identify associated Incidents prior to their Resolution, the Supplier is required to re-categorise Master Incidents as Linked Incidents if a connection is later made.

2.2.10 In the event that the Supplier categorises Incidents as Linked Incidents and then later determines that the relevant Incidents were not in fact Linked Incidents, the Supplier shall amend the Incident Record and, at the Customer's request, recalculate any impacted Service Levels and resubmit any incorrect reports to reflect this.

2.3 Severity Levels



2.3.1 All Linked Incidents must have the same Severity Level as the related Master Incident. Changes to the Master Incident's recorded Severity Level shall be reflected in the related Linked Incident's recorded Severity Level.

2.3.2 In the event that two or more Linked Incidents are allocated different Severity Levels, the applicable Severity Level for all Master Incidents and Linked Incidents shall be deemed to be the highest Severity Level allocated to any Master or Linked Incident (as the case may be).

2.3.3 In the event that the Supplier refers an Incident to another nominated supplier of the Customer, the Supplier is responsible for:

- (a) ensuring that the other supplier's minimum data set requirement for Incident logging is met for each separately referred Incident;
- (b) for notifying the Customer of the referral of their Incident to another supplier; and
- (c) Ensuring the Incident is accepted.

2.3.4 At the request of the Customer, the Supplier shall provide justification for the allocation of a particular Severity Level to an Incident. If the Customer using the Severity Level Guidelines determines that the Supplier has wrongly allocated the Severity Level to an Incident, the Customer may require the Supplier to change the Severity Level of the Incident at any time (and require the Supplier to recalculate the Service Level and Service Credits (if applicable)).

2.3.5 In the event that the appropriate Incident Severity Level cannot be agreed, the Customer will work collaboratively with the Supplier to agree the Incident Severity Level and ensure that the Incident Severity Level applicable to future occurrences of the same Incident is pre-agreed.

2.4 High Severity Service Incidents

2.4.1 The Supplier shall implement a procedure for the management and communication of HSSIs, recognising their impact upon the Customer which aligns to the handling of Support Communications.

2.4.2 The Supplier shall inform the Customer's Service Bridge as soon as possible and in any event within twenty (20) minutes of any Incidents assigned a Severity Level 1 or 2 by telephone or method agreed by the Customer and Supplier.

2.4.3 Further updates on the progress and Resolution of such Incidents shall be provided to the Customer's Service Bridge;

- (a) every 60 (sixty) minutes for a Severity 1 Incident; or
- (b) every 90 (ninety) minutes for a Severity 2 Incident, unless otherwise requested by the Customer.



2.4.4 The Supplier shall provide the Customer with a High Severity Service Incident report within 48 hours following the resolution of each HSSI and a Root Cause Analysis report within 10 working days.

2.4.5 Once the HSSI is resolved, the Supplier and Customer will undertake a post-HSSI review with the aim of preventing further Incidents.

3. Service Change Management

3.1 The Supplier and the Customer shall work together to agree a Change Management Process within 60 days of the Order Form signature date.

3.2 The Parties shall ensure that all Changes are managed in accordance with the agreed Change Management Process.

3.3 The Supplier shall provide the Customer with a forward schedule of change, detailing the planned RFCs, on a weekly basis.

3.4 The Supplier shall provide supporting information and documentation where reasonably requested from the Customer to support any RFC.

3.5 The Parties shall attend regular Change Advisory Boards to seek approval to RFCs from its customers, that approval not to be unreasonably withheld.

3.6 If an Emergency Change is required, i.e. not one identified through the forward schedule of Change, either party may request a meeting of the Emergency Change Advisory Board to seek approval for the Change.

3.7 A Change with a material clinical safety impact will require the approval of the Customer's Clinical Safety Officer in accordance with ISB 0129 Patient Safety Risk Management System – Manufacture of Health Software.

3.8 The Supplier shall ensure that all Changes are carried out in such a manner as to minimise the impact to Customer and any service recipients including the impact of the Change on the Customer's other IT services.

4. Maintenance and Release Management

4.1 The Supplier will work together with the Customer to agree a Release Management Process within 60 days of the Call Off Commencement Date that supports both Parties.

4.2 Any Release or Maintenance activity shall be carried out in such a manner as to avoid any disruption to Services and at such times as to minimise the risk of any impact to the Services.

4.3 The Supplier shall provide the Customer a Release and Maintenance Plan on a monthly basis.

4.4 The Supplier shall hold a monthly Release and Maintenance review with the Customer (and other customers) to discuss the proposed Release and Maintenance Plan and content of each Release.



- 4.5 For each Release the Supplier will issue a Release note to the Customer detailing the contents of the Release and any Defects.
- 4.6 A Release with a material clinical safety impact will require the approval of the Customer's Clinical Safety Officer in accordance with ISB 0129 Patient Safety Risk Management System – Manufacture of Health Software.
- 4.7 A Release or Maintenance activity shall be carried out in accordance with the Release and Maintenance Plan unless:
- 4.7.1 the Supplier has provided the Customer with not less than seven (7) days' written notice of a cancellation or a postponement; or
 - 4.7.2 the Customer has provided the Supplier with not less than seven (7) days' written notice which reasonably requests an alternative date for the Release or Maintenance activity.
- 4.8 If either the Supplier or the Customer postpones a Release or Maintenance activity, the Parties shall agree an alternative date for the relevant Release or Maintenance activity.
- 4.9 The Customer agrees that if it prevents the Supplier from implementing a Release or Maintenance activity, or requires a postponement in the implementation of a Release or Maintenance activity, the Supplier shall not be liable in respect of any failure to achieve a Service Level where such failure is attributable to such prevention or postponement.

5. Problem Management

5.1 Creating & Maintaining Problem Records

- 5.1.1 The Supplier shall raise a Problem Record on the Service Management Toolset as soon as:
 - (a) the Supplier becomes aware of a Problem affecting one or more of its Services (or part thereof); or
 - (b) the Supplier is notified about a Problem affecting one or more of its Services (or part thereof) by the Customer where a Problem should have already been raised under the provisions of this Call Off Schedule; or
 - (c) where the Root Cause of an Incident is unknown or requires further investigation.
- 5.1.2 The Supplier shall only raise one Problem Record for each Problem (representative of all affected Services).
- 5.1.3 The Supplier shall be deemed to be aware of, and is responsible for Logging, Problems identified by the following sources:
 - (a) via both reactive and proactive Problem management methods (through the use of performance monitoring and trending);



- (b) from Defects developing into Problems as a result of Releases or Changes being deployed; and
- (c) where an Incident has been Resolved via the use of a workaround and the underlying Root Cause is not known, a Problem Record will be Logged immediately upon closure of the Incident in any of the following circumstances:
- (d) from problems received from other suppliers; and
- (e) at the request of the Customer.

5.1.4 In relation to each Problem, the Supplier is responsible for:

- (a) allocating the Problem with a Severity Level;
- (b) assessing which Services are affected by the Problem (and updating this throughout the lifecycle of the Problem); and
- (c) monitoring and updating the Severity Level of a Problem as required, in accordance with the Severity Level Guidelines.

5.1.5 At the request of the Customer or its representative, the Supplier shall provide justification for the allocation of a particular Severity Level to a Problem. If the Customer using the Problem Severity Level Guidelines determines that the Supplier has wrongly allocated the Severity Level of a Problem, the Customer may require the Supplier to change the Severity Level of the Problem at any time (and require the Supplier to recalculate the Service Level and Service Points (if applicable)).

5.1.6 In the event that the appropriate Problem Severity Level cannot be agreed, the Customer will work collaboratively with the Supplier to agree the Problem Severity Level and ensure that the Problem Severity Level applicable to future occurrences of the same Problem is pre-agreed.

5.1.7 The Supplier shall record the reason for any change to the Severity Level that is made to a Problem Record.

5.1.8 A Problem Record shall only be closed when all components impacted by the relevant Problem have received a Permanent Fix and the Customer confirms acceptance to the Supplier.

5.1.9 Upon request, the Supplier shall update the Customer about any aspects of a Problem.

5.1.10 The Supplier will be responsible for the provision and upkeep of a Customer facing Problem Management database report.

5.1.11 The Supplier should make available a copy of its Problem tracker on a weekly basis. The tracker will list details of every problem record irrespective of status which is recorded by the Supplier; in addition to this the Supplier



will provide monthly problem related KPI statistics within 2 working days of the end of each month. This will include the number of Problems opened that month, the number of Problems closed that month, the average age of open problems at the end of that month and the total number of open problem records

5.2 Problem Management – Known Errors

- 5.2.1 The Supplier shall conduct Root Cause analysis for each Problem Record in order to identify a Known Error and subsequently robust resolution for each and ensure that the Root Cause is fully understood prior to the development of any fix.
- 5.2.2 The Supplier will facilitate the Resolution of Known Errors via the Supplier's Change Management Process and release management process.
- 5.2.3 The Supplier shall make Known Errors relating to Problems available to the Supplier's Incident Management teams in order to match them to Incidents.

Customer's ICT and Security Policy

Where the Supplier is required to comply with the Customer's ICT Policy and Security Policy then append to this Order Form as a clearly marked document

Security Management Plan

Where the Supplier is required to provide the Customer with the Security Management Plan then append to this Order Form as a clearly marked document

Section C **Customer Core Services Requirements**

Please provide details of all Services required including the locations where the Supplier is required to provide the Services Ordered.

Services

List below or append as a clearly marked document to confirm the Services which the Supplier shall provide to the Customer (which could include the Customer's requirement and the Supplier's response to the Further Competition Procedure)

The Supplier shall provide the Services in accordance with the Statement of Works set out in Section D of this Order Form.

The following terms are not applicable as at the Call Off Commencement Date as no Supplier Software is being provided. In the event Supplier Software is provided during the Term in respect of Services provided under this Call Off Contract, Supplier will use reasonable endeavours to include the terms set out below in the licence terms for any Supplier Software provided, subject to Variation.

- 1 The following requirements shall take priority above all terms, conditions and specifications set out in this Call Off Contract (including without limitation any embedded documents and terms),



and the Supplier shall ensure that the software licences meet and conform with the following requirements:

1.1 The Customer shall be entitled, free of charge, to sub licence the software to any contractor and/or Sub-Contractor of the Customer who is working towards and/or is providing services to the Customer.

1.2 The Customer's role as national information and technology partner to the NHS and social care bodies involves the Customer buying services for or on behalf of the NHS and social care entities. Nothing in the licences for any of the software shall have the effect of restricting the Customer from discharging its role as the national information and technology partner for the health and care system, which includes the ability of the Customer to offer software and services to the NHS and social care entities. Specifically, any software licensing clause prohibiting 'white labelling', 'provision of outsourcing services' or similar, shall not be interpreted as prohibiting the Customer's services.

1.3 The Customer shall be entitled to deploy the software at any location from which the Customer and/or any contractor and/or Sub-Contractor of the Customer is undertaking services pursuant to which the software is being licenced.

1.4 Any software licenced to the Customer on a named user basis shall permit the transfer from one user to another user, free of charge provided that the Supplier is notified of the same (including without limitation to a named user who is a contractor and/or Sub-Contractor of the Customer).

1.5 The Supplier shall ensure that the Customer shall be entitled to assign or novate all or any of the software licences free of charge to any other central government entity, by giving the licensor prior written notice.

1.6 The Supplier shall notify the Customer in advance if any software or service permits the Supplier or any third party remote access to the software or systems of the Customer.

1.7 Where the Supplier is responsible for the calculation of the appropriate number of users for software, and it is later shown there is a shortfall of licences, the Supplier shall be responsible for all costs of the Customer.

Location/Site(s) for provision of the Services

The Services will be delivered remotely by the Supplier however the Supplier shall comply with requests by the Customer to co-locate with the Customer in London where required.

Additional Clauses (see Annex 3 of Framework Schedule 4)

This Annex can be found on the RM3804 CCS webpage. The document is titled RM3804 Additional Clauses.

Those Additional Clauses selected below shall be incorporated into this Call Off Contract

Applicable Call Off Contract Terms

Optional Clauses

Can be selected to apply to any Order

Additional Clauses and Schedules



Tick any applicable boxes below

A: SERVICES – Mandatory

The following clauses will automatically apply where Lot 3 services are provided (this includes Lot 4a & 4b where Lot 3 services are included).



A3: Staff Transfer

A4: Exit Management

A: PROJECTS - Optional

Only applies to Lots 1 and 2

A1: Testing



A2: Key Personnel



B: SERVICES - Optional

Only applies to Lots 3 and 4a and 4b

B1: Business Continuity and Disaster Recovery



B2: Continuous Improvement & Benchmarking



B3: Supplier Equipment



B4: Maintenance of the ICT Environment



B5: Supplier Request for Increase of the Call Off Contract Charges



B6: Indexation



B7: Additional Performance Monitoring Requirements



Tick any applicable boxes below

C: Call Off Guarantee



D: Relevant Convictions



E: Security Requirements



F: Collaboration Agreement

Where required please complete and append to this Order Form as a clearly marked document (see Call Off Schedule F)



G: Security Measures



H: MOD Additional Clauses



Alternative Clauses

To replace default English & Welsh Law, Crown Body and FOIA subject base Call Off Clauses

Tick any applicable boxes below

Scots Law
Or



Northern Ireland Law



Non-Crown Bodies



Non-FOIA Public Bodies



Collaboration Agreement (see Call Off Schedule F) This Schedule can be found on the RM3804 CCS webpage. The document is titled RM3804 Call Off Schedule F.

An executed Collaboration Agreement shall be delivered from the Supplier to the Customer within

N/A.



Organisations required to collaborate (Collaboration Suppliers)
N/A.

the stated number of Working Days from the Call Off Commencement Date *insert right*
OR

An executed Collaboration Agreement from the Supplier has been provided to the Customer and is attached to this Order Form.
tick box (right) and append as a clearly marked complete document

☐

Licensed Software Where Software owned by a party other than the Customer is used in the delivery of the Services list product details under each relevant heading below

Supplier Software

None.

Third Party Software

Own{backup}

Salesforce products:

Health Cloud Service UE

myTrailhead

Partner Community Licence

Customer Community Cloud Members
plus for Health Cloud Licence

Salesforce Shield

Data Masking

Mulesoft

Customer Property *(see Call Off Clause 21)*

Items licensed by the Customer to the Supplier (including any Customer Software, Customer Assets, Customer System, Customer Background IPR and Customer Data)

List below if applicable

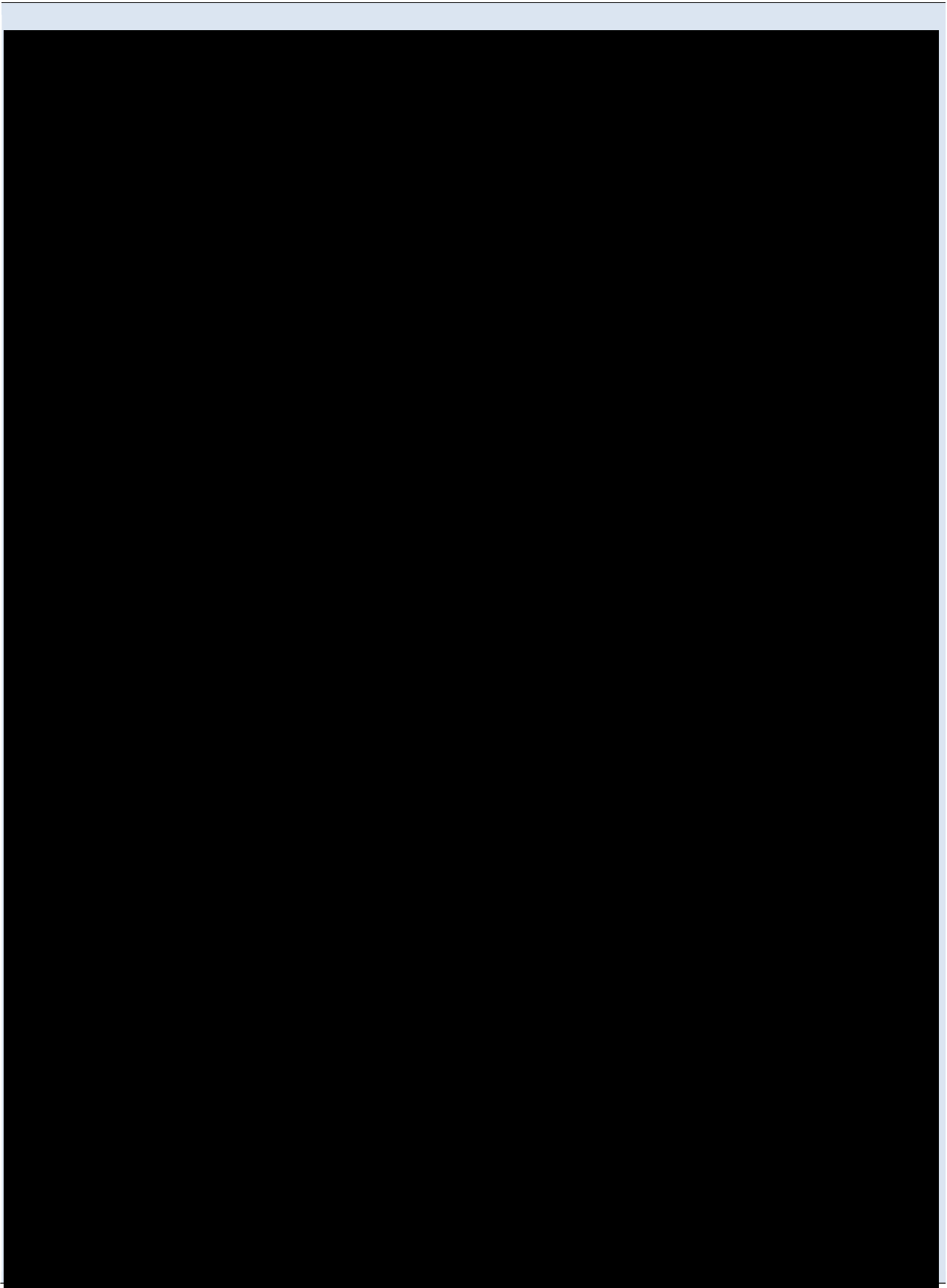
None.

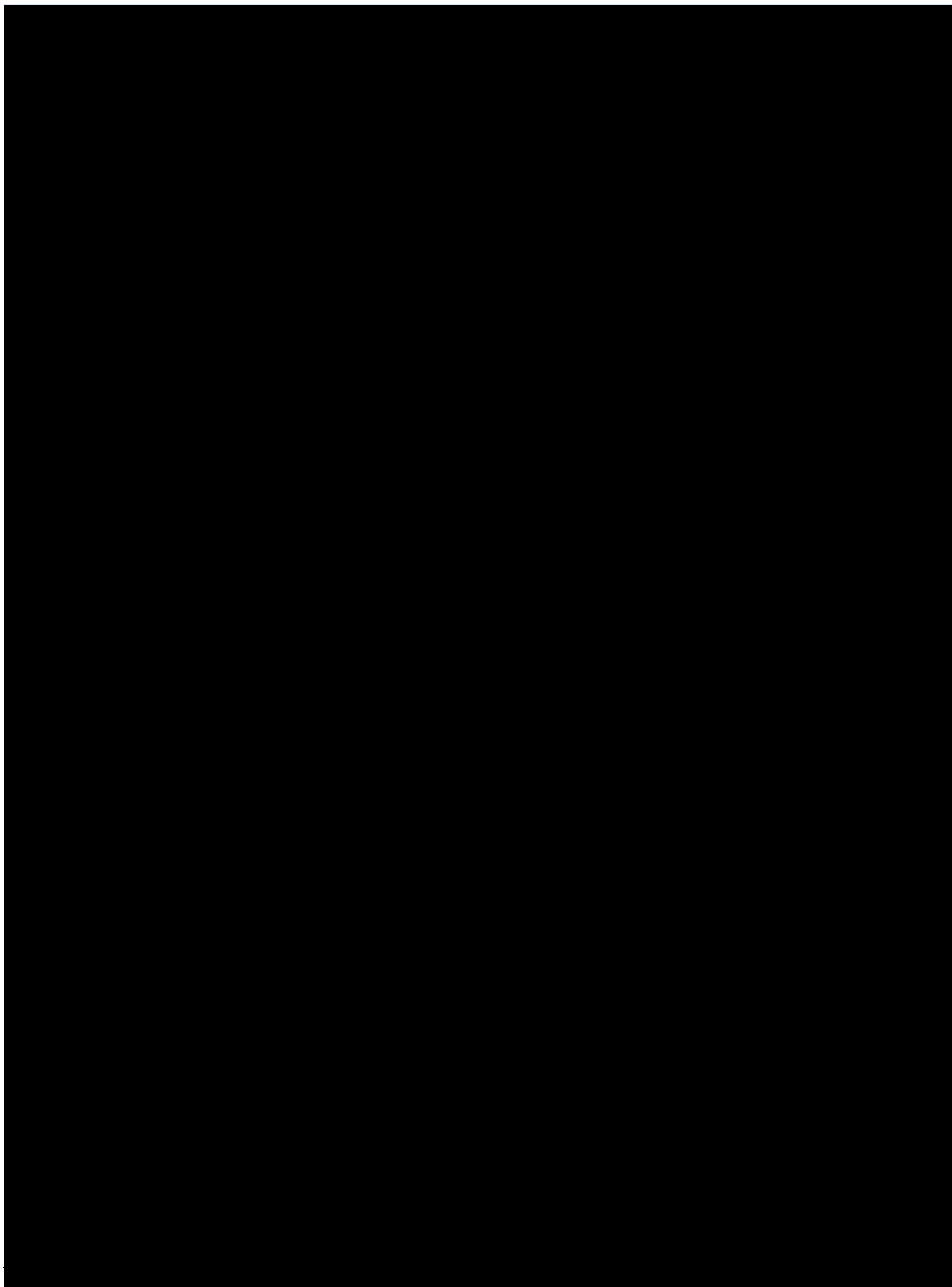
Call Off Contract Charges and Payment Profile *(see Call Off Schedule 2)*

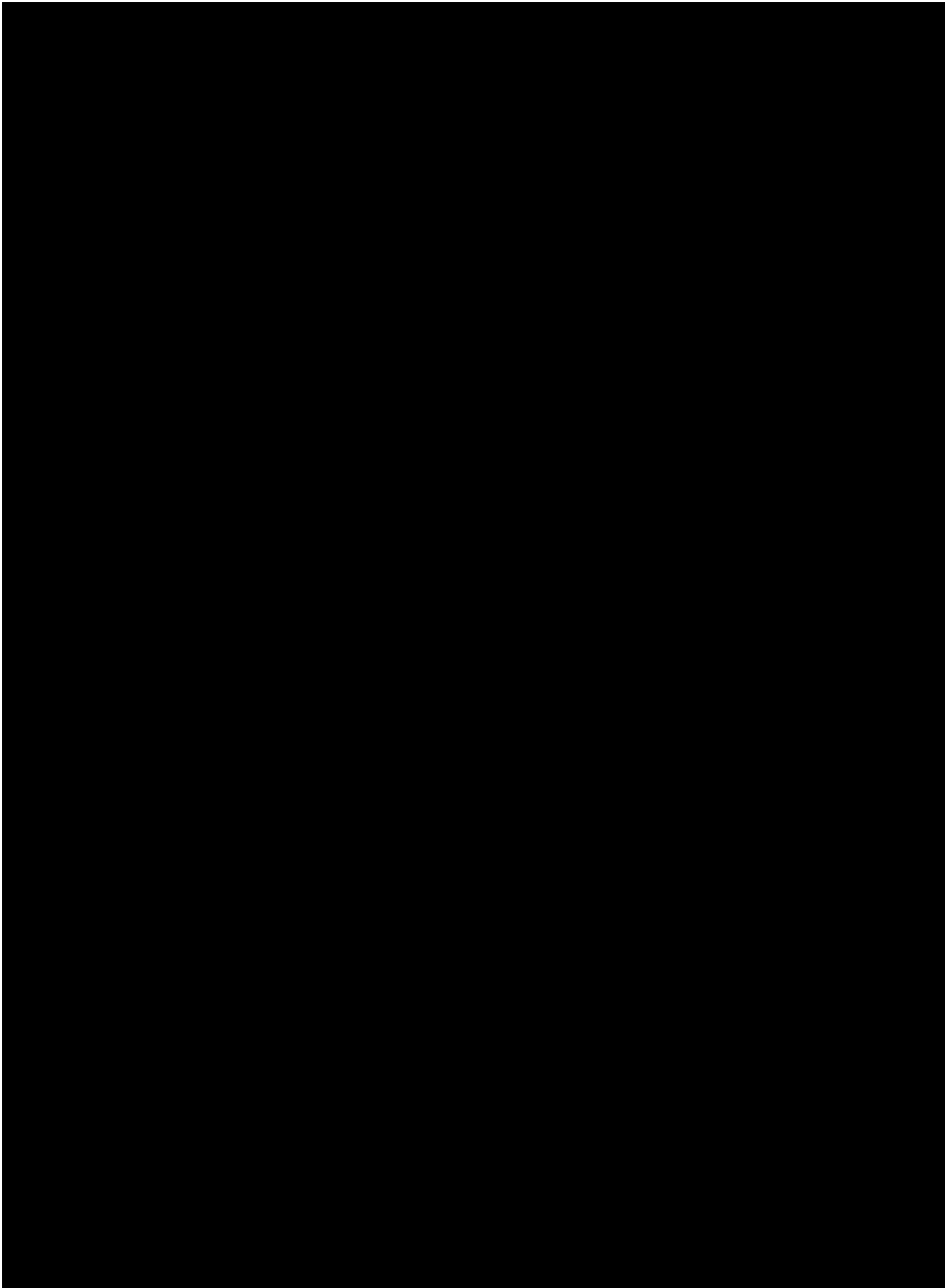
Include Charges payable by the Customer to the Supplier (including any applicable Milestone Payments and/or discount(s), but excluding VAT) and payment terms/profile including method of payment (e.g. Government Procurement Card (GPC) or BACS)

List below or append as a clearly marked document

The Charges which are applicable to this Order Form are set out below:



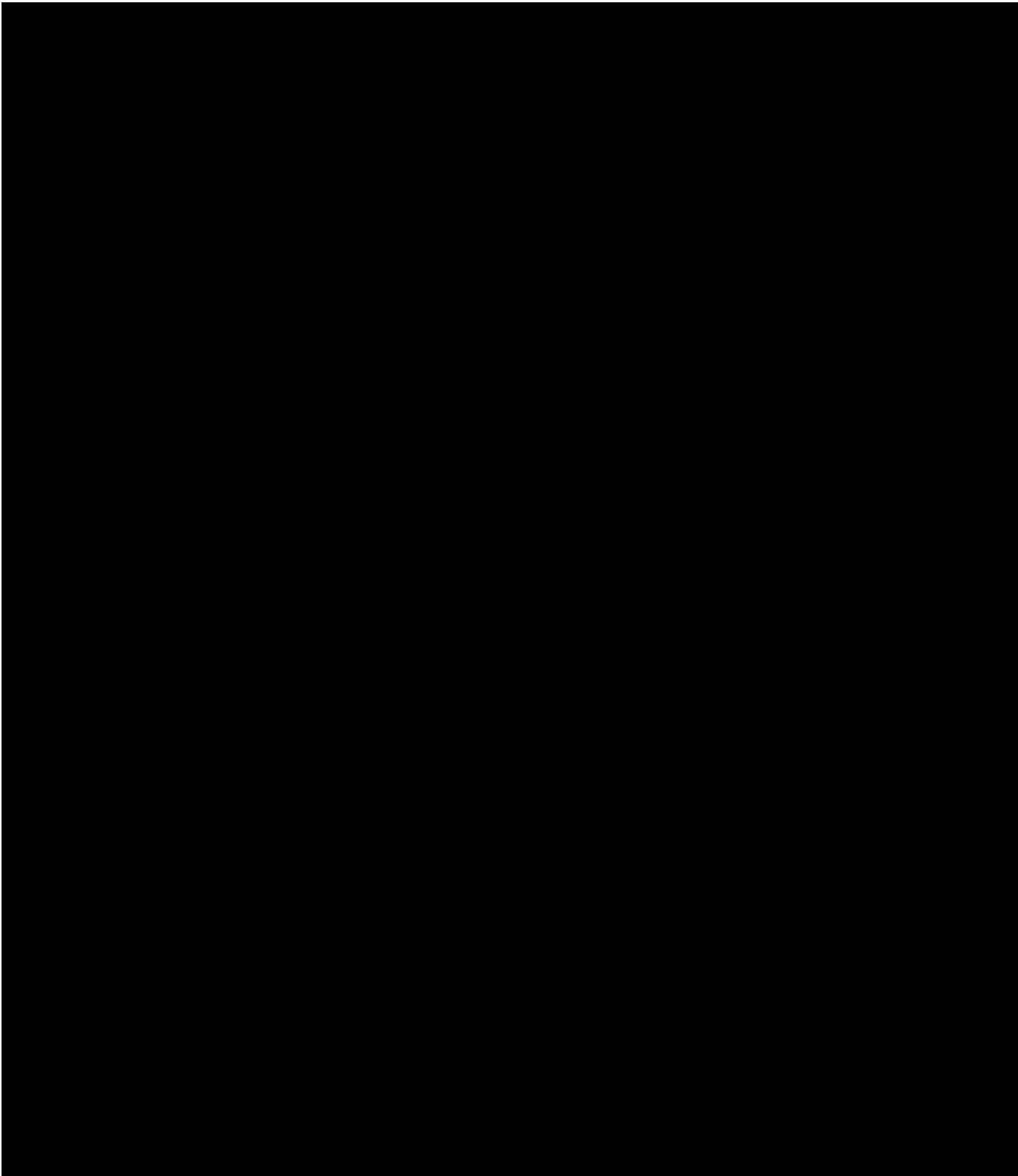






****Additional work packages (statement of works ("SOW's")) will be completed using the Variation Procedure aligned to Schedule 15 of the Call of Terms and Conditions and shall be based on the Contract Charges as set out in this Order Form. In the event of any conflict between the Order Form and any SOWs, the terms of this Order Form shall take precedence over the terms of the SOWs.***

Supplier Personnel Rate Card



Undisputed Sums Limit (£)

Insert right (see Call Off Clause 31.1.1)

N/A

Delay Period Limit (calendar days)

Insert right (see Call Off Clause 5.4.1(b)(ii))

N/A



Estimated Year 1 Call Off Contract Charges (£)

For Call Off Contract Periods of over 12 Months

Enhanced Insurance Cover

Where a specific Call Off Contract requires a higher level of insurance cover than the £1m default in Framework Schedule 14 please specify below

Third Party Public Liability Insurance (£)

Professional Indemnity Insurance (£)

Transparency Reports (see Call Off Schedule 6)

If required by the Customer populate the table below to describe the detail (titles are suggested examples)

Title	Content	Format	Frequency
Service Performance Report	To be defined and agreed with the Customer	To be defined and agreed with the Customer	Monthly
Call Off Contract Charges Report	To be defined and agreed with the Customer	To be defined and agreed with the Customer	Monthly
Project Status Report	To be defined and agreed with the Customer	To be defined and agreed with the Customer	Weekly
MI Report	As set out in the MI Reporting Template included in Paragraph 14A of the Call Off Terms	As set out in the MI Reporting Template included in Paragraph 14A of the Call Off Terms	Monthly

Quality Plans (see Call Off Clause 7.2)

Time frame for delivery of draft Quality Plans from the Supplier to the Customer – from the Call Off Commencement Date (Working Days)

Where applicable insert right

10 calendar days from the (latest) signature date of the Order Form

Implementation Plan (see Call Off Clause 5.1.1)

Time frame for delivery of a draft Implementation Plan from the Supplier to the Customer – from the Call Off Commencement Date (Working Days)

Where applicable insert right

10 calendar days from the (latest) signature date of Order Form

BCDR (see Call Off Schedule B1)

This can be found on the CCS RM3804 webpage. The document is titled RM3804 Additional Clauses.



An executed BCDR Plan from the Supplier is required prior to entry into the Call Off Contract tick box (right) and append as a clearly marked complete document

OR



Time frame for delivery of a BCDR Plan from the Supplier to the Customer – from the Call Off Commencement Date (Working Days) Prior to Go Live of the MVP
Where applicable insert right

Disaster Period (calendar days) 3 calendar days

GDPR (see Call Off Clause 23.6)

Where a specific Call Off Contract requires the inclusion of GDPR data processing provisions, please complete and append Call Off Schedule 7 to this order form. This Schedule can be found in the Call Off Contract on the RM3804 CCS webpage

Supplier Equipment (see Call Off Clause B3)

This can be found on the RM3804 CCS webpage. The document is titled RM3804 Additional Clauses.

X - Service Failures (number)

Where applicable insert right

N/A

Y – Period
(Months)

*Where applicable
insert right*

N/A.

Key Personnel & Customer Responsibilities (see Call Off Clause A2)

List below or append as a clearly marked document to include Key Roles

Key Personnel

List below or append as a clearly marked document to include Key Roles

Customer Responsibilities

List below or append as a clearly marked document

Please see Section D of this Order Form.

Relevant Conviction(s)

Where applicable the Customer to include details of Conviction(s) it considers relevant to the nature of the Services.

List below or append as a clearly marked document (see Call Off Clause D where used)

N/A.

Appointment as Agent (see Call Off Clause 19.5.4)

Insert details below or append as a clearly marked document

Specific requirement and its relation to the Services

N/A.

Other CCS framework agreement(s) to be used

N/A.



SERVICE LEVELS AND SERVICE CREDITS (see Part A of Call Off Schedule 3)

Service Levels

If required by the Customer populate the table below to describe the detail (content is suggested examples)

Service Level Performance Criteria	Key Indicator	Service Level Performance Measure (measured across a Service Period)	Service Credit for each Service Period
Change Management - Time to Execute Changes – End to end time to execute changes to the solution in-line with the Change Management Process (to be defined).	Performance	[REDACTED] of changes implemented to the agreed plan as defined in the approved change request (as defined in the Change Management Process) – measured on a calendar month.	[REDACTED] Service Credit gained for each percentage under the specified Service Level Performance Measure.
Time to Fix/Execute The time taken to fix the Incident from the point of the Supplier being notified (automatically or via a report). This Service Level applies to Incidents where the Root Cause is solely due to the Supplier.	Performance	% of calls not fixed within the Service Level detailed below vs total number of Incidents broken down by Severity Level Severity Levels - max time to fix: Severity 1 (2 hours) - [REDACTED] Severity 2 (4 hours) – [REDACTED] Severity 3 (16 hours) [REDACTED] Severity 4 (48 hours) [REDACTED] See Severity Level Guidance for definitions.	[REDACTED] Service Credit gained for each percentage under the specified Service Level Performance Measure for severity level 1 and severity level 2 ----- [REDACTED] Service Credit gained for each percentage under the specified Service Level Performance Measure for severity level 3 ----- [REDACTED] Service Credit gained for each percentage under the specified Service Level Performance Measure for severity level 4
Customer Notification Time The time taken to notify the Customer of Incident from the	Performance	% of calls not reported / notified within the Service Level detailed below vs total number of Incidents broken	None



point of the Incident being notified to the Supplier or the Supplier becoming aware.		<p>down by Severity Level.</p> <p>Severity Levels - max time to fix:</p> <p>Severity 1 (15 Mins) - [REDACTED]</p> <p>Severity 2 (30 Mins) – [REDACTED]</p> <p>Severity 3 (1 hour) – [REDACTED]</p> <p>Severity 4 (4 hours) – [REDACTED]</p> <p>See Severity Level Guidance for definitions.</p>	
<p>Third Party Notification Time</p> <p>The time taken to notify the third parties of an Incident from the point of the Incident being notified to the Supplier or the Supplier becoming aware that the Incident is within the third party solution.</p>	Performance	<p>% of calls not reported / notified within the Service Level detailed below vs total number of Incidents broken down by Severity Level.</p> <p>Severity Levels - max time to fix:</p> <p>Severity 1 (15 Mins) - [REDACTED]</p> <p>Severity 2 (30 Mins) – [REDACTED]</p> <p>Severity 3 (4 hour) – [REDACTED]</p> <p>Severity 4 (8 hours) – [REDACTED]</p> <p>See Severity Level Guidance for definitions.</p>	None

Service Levels

1. The Services shall be measured against the Service Levels and rated with a standard of service as set out below:
 - 1.1. the expected level of service (“Operating Service Level” or “OSL”);



- 1.2. the level at which the Supplier fails to achieve the Operating Service Level and Service Credits, where relevant, begin to accrue ("Failure Level " or "FL3");
- 1.3. an unacceptable level of service ("Critical Service Level" or "CSL") and where relevant, where the Supplier shall accrue maximum Service Credits available to that Service Level.
2. The Supplier shall ensure the Services meet or exceeds the OSL against each Service Level for each Month.

Time to Fix/Execute Service Level

	Details of Service Level: Fix Times for Severity 1 Incidents. Standard Required
OSL	<= 2 hours
CSL	> 2 hours

	Details of Service Level: Fix Times for Severity 2 Incidents. Standard Required
OSL	<= 4 hours
FL3	> 4 hours

	Details of Service Level: Fix Times for Severity 3 Incidents. Standard Required
OSL	<= 16 hours
FL3	> 16 hours

	Details of Service Level: Fix Times for Severity 4 Incidents Standard Required
OSL	<= 48 hours
FL3	>48 hours

Severity Level Guidance

Notwithstanding the following examples, (provided for information only), the Parties acknowledge that the Severity Levels appropriate to the Services under the Call Off Contract will be set out in the Process Interface Manual (PIM) and will take precedence over the examples in the table below.

Severity	Description
1	<p>Loss of the Service or major functional or non-functional issue which results in either a) the complete service being unusable by a majority of agents, or b) a significant element of the service being unusable by all agents or direct website users.</p> <p>Examples of which (but not an exhaustive list) are:</p> <ul style="list-style-type: none"> Have significant adverse impact on the provision of service to a large number of agents



	<ul style="list-style-type: none">• Have significant adverse impact on the delivery of patient care to a large number of patients• Causes significant financial loss and/or disruption to the Customer• Result in any material loss or corruption of Customer Data or in the provision of incorrect Customer Data
2	<p>Significant issue with the Service (functional or non-functional) which deems a significant element of the service unusable to a number of agents or direct website users.</p> <p>Examples of which (but not an exhaustive list) are:</p> <ul style="list-style-type: none">• Have significant adverse impact on the provision of service to a small (i.e. one or more) or moderate number of agents• Have moderate adverse impact on the delivery of patient care to a large number of End Users• Have significant adverse impact on the delivery of patient care to a small (i.e. one or more) or moderate number of patients• Have a moderate adverse impact on the delivery of patient care to a high number of patients• Causes financial loss and/or disruption to the Customer which is more than trivial but less severe than the significant financial loss described in the definition of severity 1• Result in any loss or corruption of Customer Data or in the provision of incorrect Customer Data
3	<p>Moderate issue with the Service (functional or non-functional) that does not render a significant element of the service unusable, but has an adverse effect on the use of the service.</p> <p>Examples of which (but not an exhaustive list) are;</p> <ul style="list-style-type: none">• Have moderate adverse impact on the provision of service to a small (i.e. one or more) or moderate number of agents• Have a minor adverse impact on the provision of the Service to a large number of agents• Have moderate adverse impact on the delivery of patient care to a small (i.e. one or more) or moderate number of patients• Have a minor adverse impact on the delivery of patient care to a large number of patients
4	<p>Minor issue with the Service that has a low impact or has a viable workaround promptly available. Minor or cosmetic issue with no functional impact.</p> <p>Examples of which (but not an exhaustive list) are:</p>



- Have a minor adverse impact on the provision of the Service to a small (i.e. one or more) or moderate number of agents

The Supplier shall provide Service Management services in accordance with the following core hours (“**Core Hours**”):

Service Management	Coverage Hours
Service Desk	8am – 8pm x 7 days
Incident Management – Severity Level 1 and 2 Incidents	24x7x365
Incident Management – Severity Level 3 Incidents	9am – 6pm Mon – Fri on Working Days + On call
Incident Management – Severity Level 4 Incidents	9am – 5pm Mon – Fri on Working Days
Problem Management – Critical Incidents	24x7x365
Problem Management – High	9am – 5pm Mon – Fri on Working Days
Problem Management – Medium	9am – 5pm Mon – Fri on Working Days
Service Optimisation support	9am – 5pm Mon – Fri on Working Days
Disaster Recovery	9am – 5pm Mon – Fri on Working Days
Change Management	9am – 5pm Mon – Fri on Working Days
Service Configuration Management	9am – 5pm Mon – Fri on Working Days
Asset Management	9am – 5pm Mon – Fri on Working Days
Patch Management	9am – 5pm Mon – Fri on Working Days

Critical Service Level Failure (see Call Off Clause 9)



Agree and specify the metrics for Critical Service Level Failures in the marked areas below

In relation to **Change Management – Time to Execute Changes Service Level** a Critical Service Level Failure shall include two or more occurrences of the Supplier failing to achieve the **Change Management – Time to Execute Changes Service Level Performance Measure** for two consecutive months, or a total of four months in any rolling 12 month period.

In relation to **Time to Fix Service Level** a Critical Service Level Failure shall include two or more occurrences of the Supplier failing to achieve the **Time to Fix Service Level Performance Measure** for two consecutive months, or a total of four months in any rolling 12 month period.

The number of Service Level Performance Criteria for the purpose of Clause 8.6 of the Call Off Terms shall be 4.

Service Credits

1. Service Credits will not apply where the volume of items is below a minimum level to mitigate the artificial effect that low volumes have on the Service Credit formula. For the avoidance of doubt, this allowance only applies to Change Requests and Time to Fix Service Levels.
 - a. In relation to Change Requests and Time to Fix incidents there must be a minimum number of service level events (the “**Minimum Event Quantity**”) measured in the Service Measurement Period, which is calculated as:
 - b. Where the target percentage for the Service Level is defined at 100%, the formula cannot be utilised and a minimum of [REDACTED] service level events (the “Minimum Event Quantity”) will apply.
 - c. In the event that the Minimum Event Quantity is not met, the measurement will roll forward until either the Minimum Event Quantity has been met or [REDACTED] have elapsed.
 - d. [REDACTED] and the Minimum Event Quantity has still not been met, then the following will apply:
 - i. If there has been [REDACTED] failures in the period, then the Service Level will be deemed to be satisfied;
 - ii. If there has been more than [REDACTED] failure, then the Service Level will be deemed to have been missed by the Supplier and the actual performance will



be calculated using the Minimum Event Quantity as the denominator and the actual failures as the numerator (see below for example):

Worked Example:

The target is 95% - therefore the Minimum Event Quantity is [REDACTED]

If in Month 1 there were [REDACTED] items, then this would roll over into Month 2.

If in Month 2 there were a further [REDACTED] items (meaning [REDACTED] items in total) then this would roll over in Month 3.

At Month 3 there are a further 3 items, resulting in a total of [REDACTED] items. The Supplier shall at this point calculate the actual performance:

If there were [REDACTED] misses out of the [REDACTED] items, the calculation would be [REDACTED] achievement [REDACTED] as the denominator as it is the Minimum Event Quantity in this example.

The [REDACTED] achievement would be assessed against any Service Credits due to the Customer. Any service credits would be paid against Month [REDACTED] Service Charges.

Service Credit Cap

Agree and specify the Service Credit Cap in the marked areas below

Additional Performance Monitoring Requirements

Technical Board (see paragraph 2 of Call Off Schedule B7) – where required

If required by the Customer populate the table below to describe the detail

Required Members			
Job Title	Name	Location	Frequency
N/A.	N/A.	N/A.	N/A.

None

Time frame in which the Technical Board shall be established – from the Call Off Commencement Date (Working Days) Where applicable insert right N/A

Exit Plan



In accordance with Schedule A4 (Exit Management) of the Call Off Terms, within three (3) months after the Call Off Commencement Date, the Supplier shall deliver to the Customer an Exit Plan which sets out the Supplier's proposed methodology for achieving an orderly transition of the Services from the Supplier to the Customer, Customer and/or its Replacement Supplier on the expiry or termination of a Call Off Contract.

The implementation of the agreed Exit Plan will be subject to additional charge as a future Variation and therefore is excluded from this Order Form.

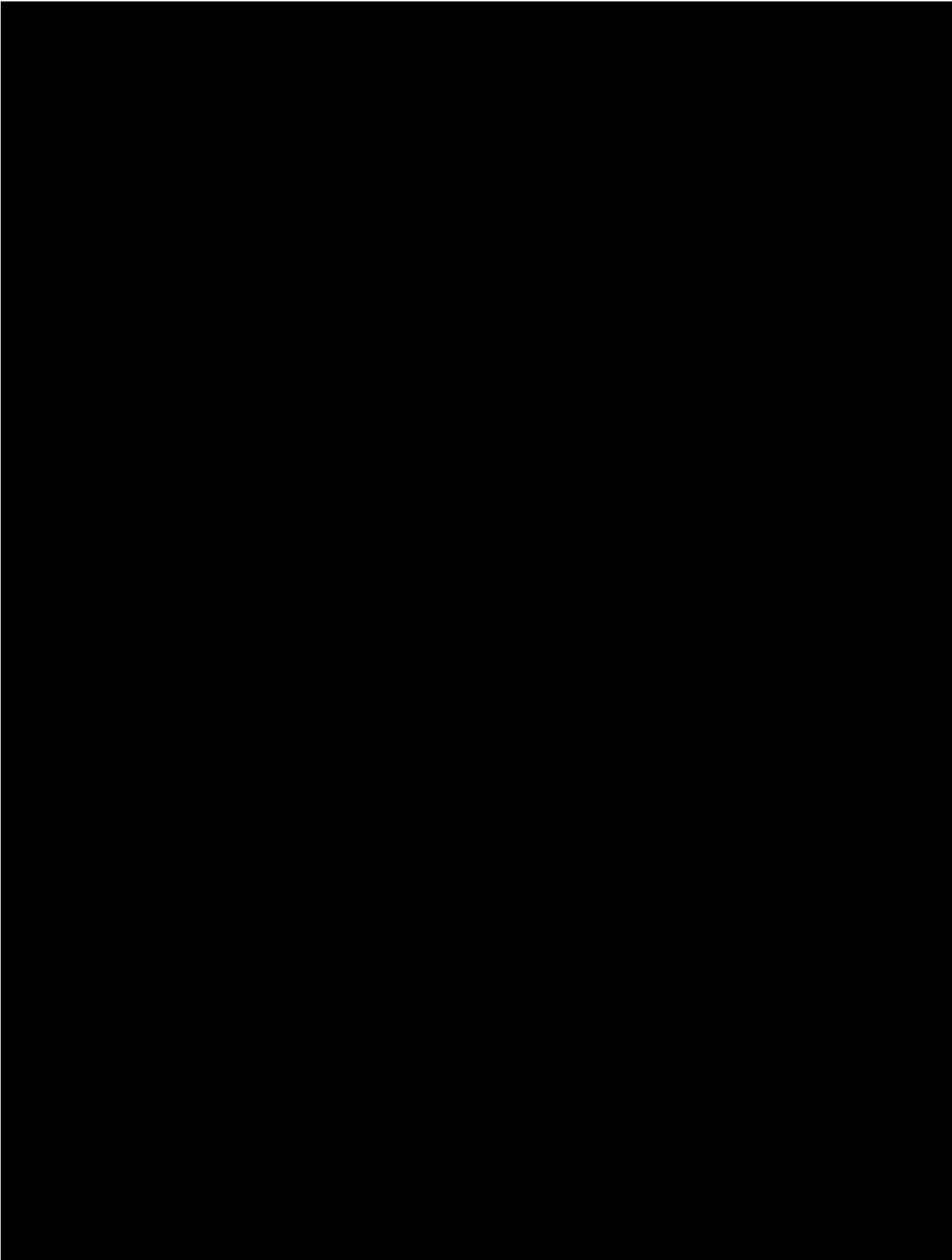


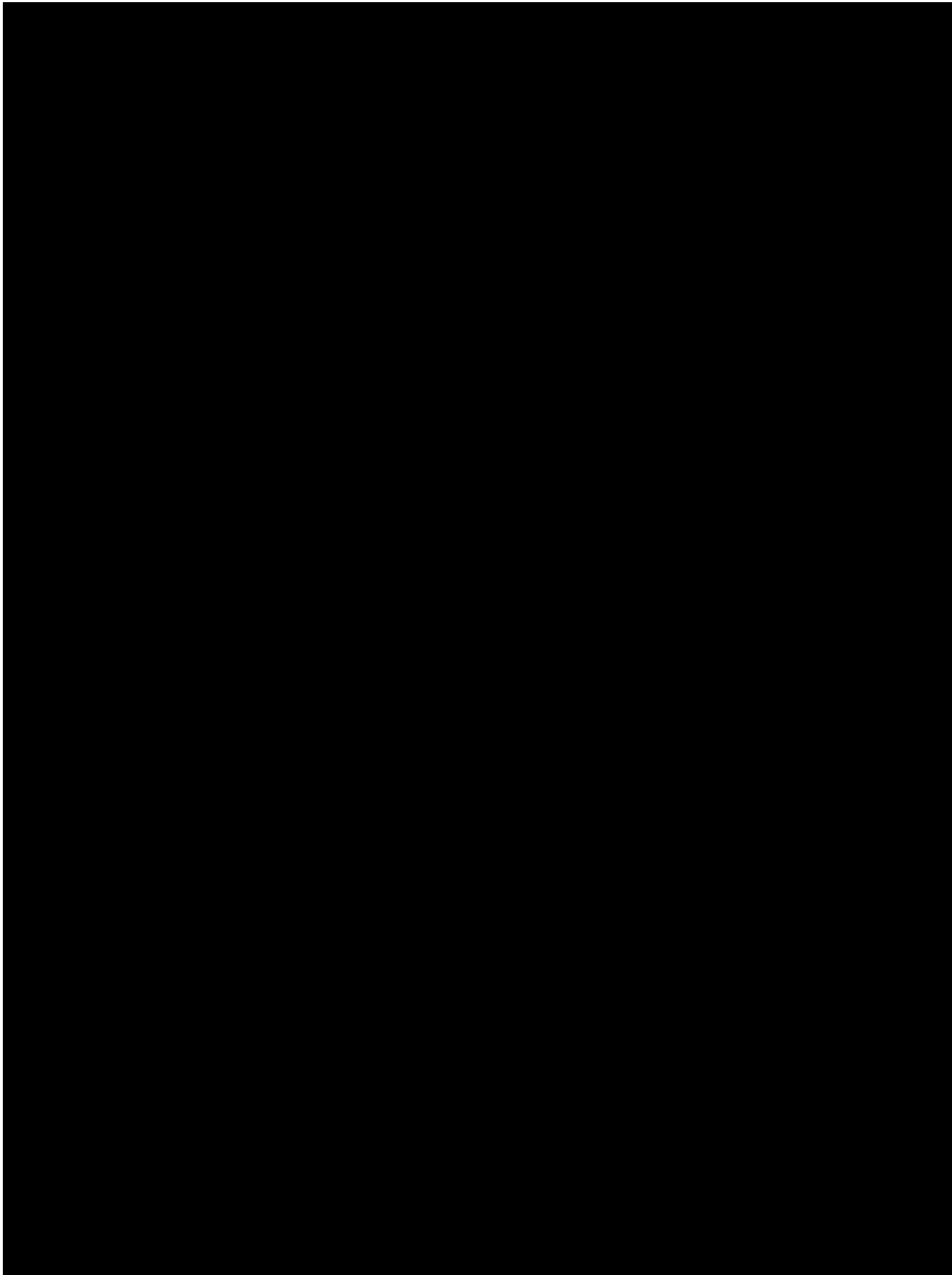
Section D

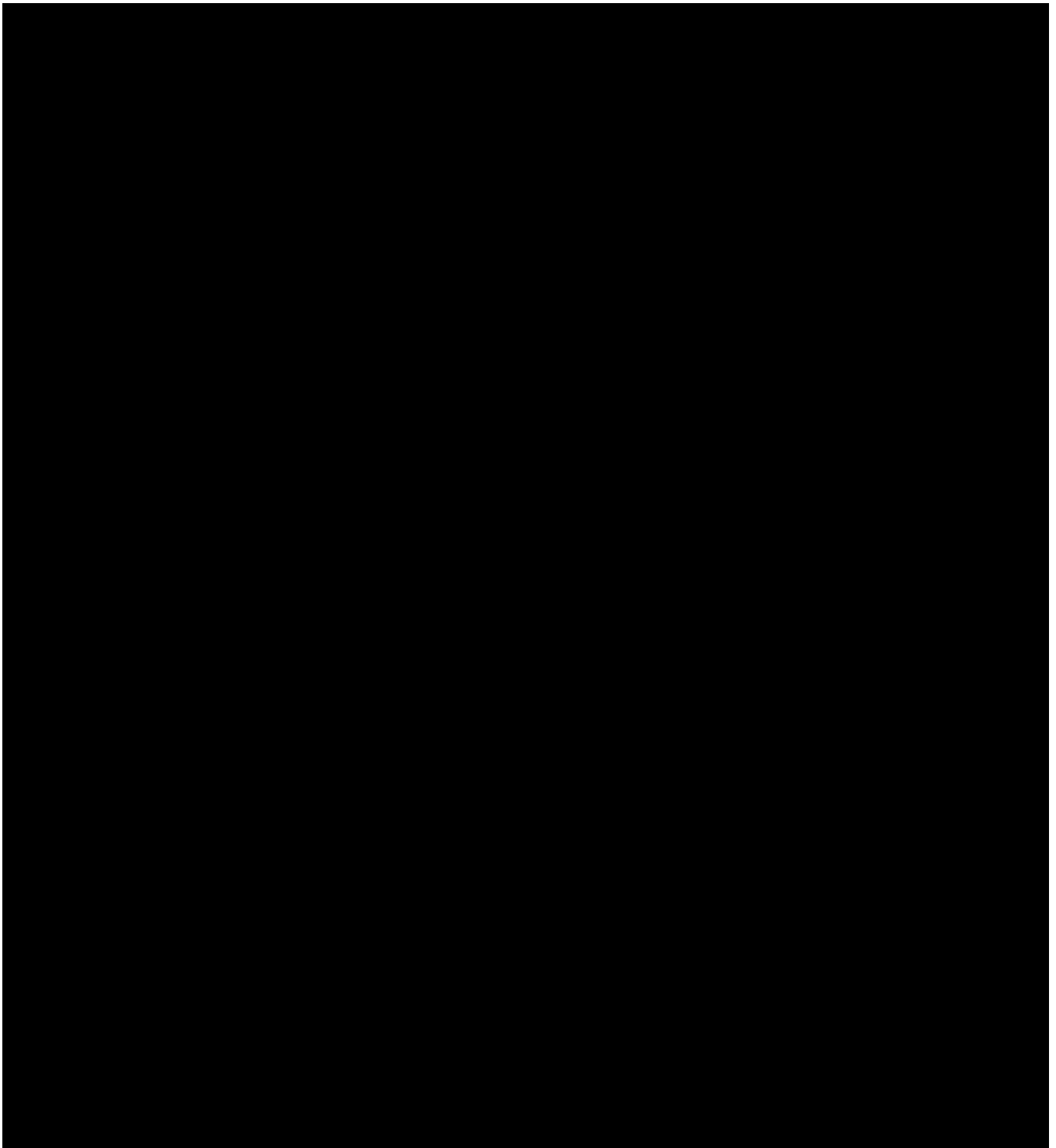
Supplier response

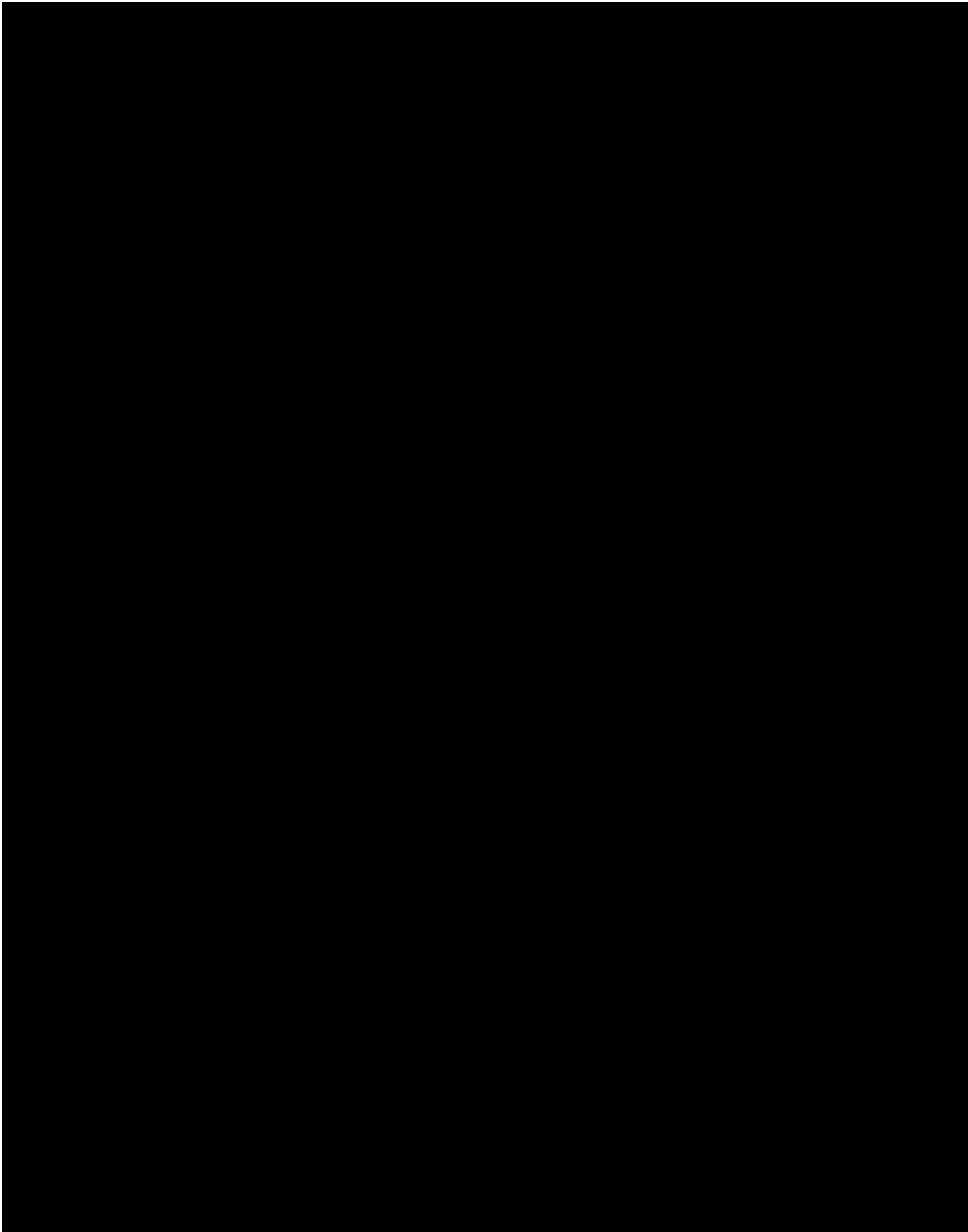
Suppliers - use this section to provide any details that may be relevant in the fulfilment of the Customer Order

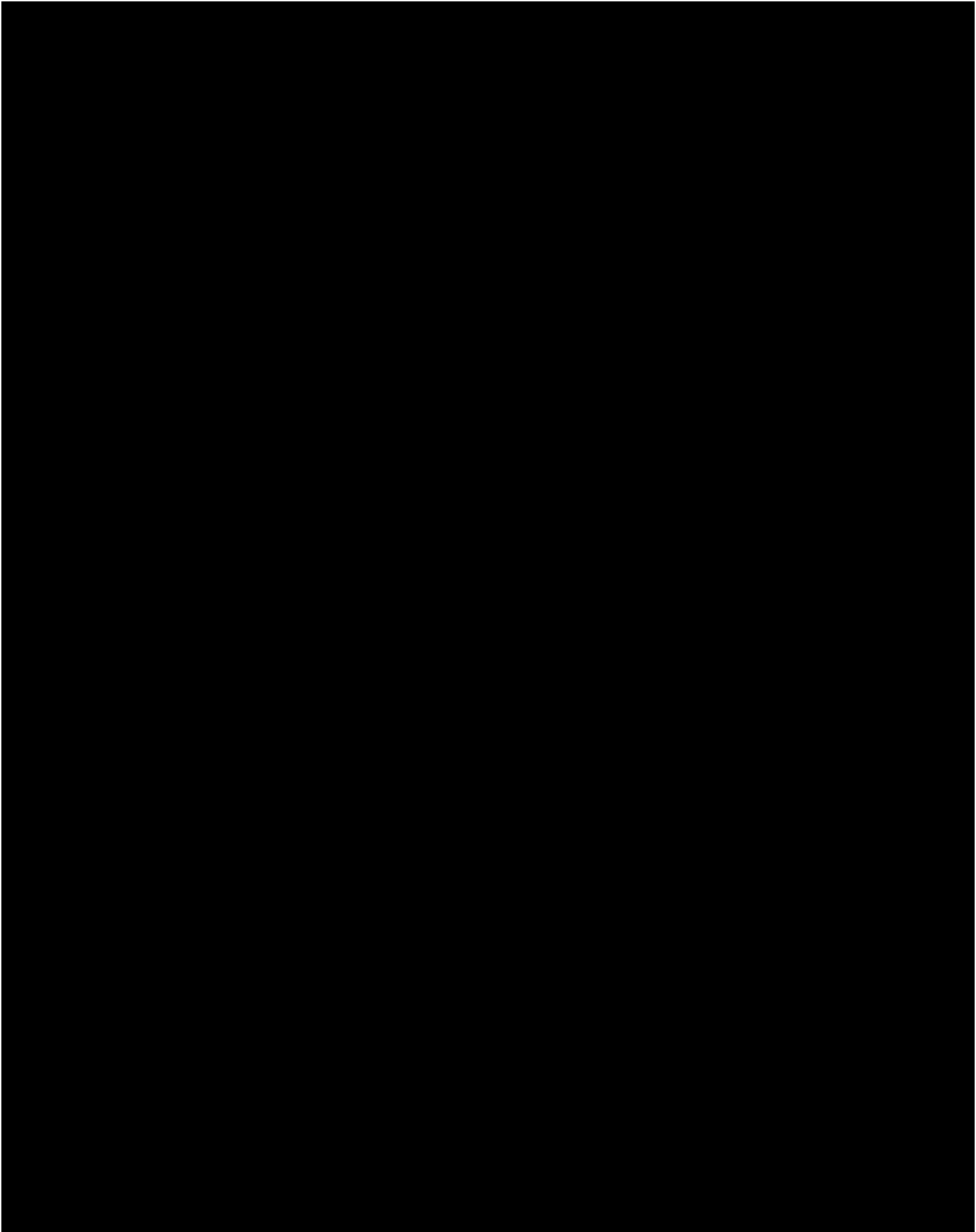
[Redacted content]

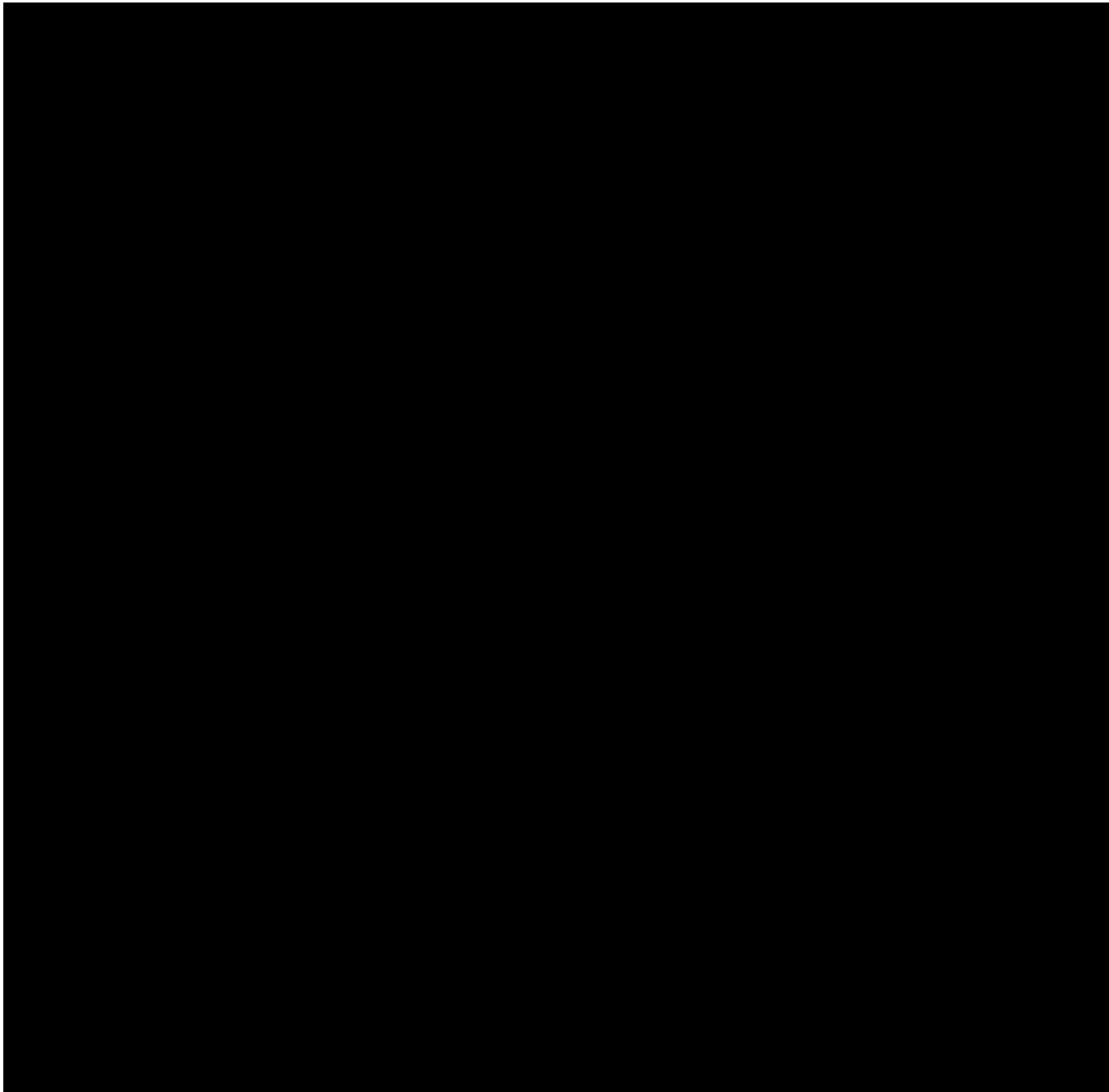












Commercially Sensitive information

Any information that the Supplier considers sensitive for the duration of an awarded Call Off Contract
All Supplier pricing information set out in the Call-Off Contract;
The details in liability and insurance clauses in the Call-Off Contract.
Value of any Service Credit cap.
Supplier ITT Response and associated tender documentation
Supplier Key Personnel

Total contract value



Crown
Commercial
Service

Please provide the total contract value (for the Call Off Initial Period) as detailed in your response to the Customer's statement of requirements
£25,000,000



Section E

Call Off Contract award

This Call Off Contract is awarded in accordance with the provisions of the Technology Services 2 Framework Agreement RM3804.

The Supplier shall provide the Services specified in this Order Form to the Customer on and subject to the terms of this Order Form and the Call Off Terms (together referred to as “the Call Off Contract”) for the duration of the Call Off Contract Period.

SIGNATURES

The individuals set out below shall execute this Call Off Contract, on behalf of the Customer and the Supplier, either using a manuscript signature or an electronic signature. A manuscript signature shall be placed in the execution block below, an electronic signature shall be evidenced in an execution block to be attached as the final page of this Order Form:

For and on behalf of the Supplier:

Name of individual signing:	[Redacted]
Title:	[Redacted]
Email:	[Redacted]
Signature (only applicable for manuscript signature):	[Redacted]
Date (only applicable for manuscript signature):	23 OCTOBER 2020



For and on behalf of the Customer:

Name of individual signing:	[Redacted]
Title:	[Redacted]
Email:	[Redacted]
Signature (only applicable for manuscript signature):	[Redacted]
Date (only applicable for manuscript signature):	22 October 2020



Annex A

Additional Terms to Customer in respect of Resold Subscription and Support Services from Salesforce

The Customer and Salesforce UK Limited (“**SFDC**”), through a Master Subscription Agreement and associated addendum together with any exhibits, schedules and documentation (as appended to this Order Form and as updated and amended in accordance with its terms) (“**MSA**”) have agreed terms and conditions that apply to and govern subscriptions and support to Salesforce services, which are to be resold by the Supplier under this Order Form (the “**Resold Subscriptions**”).

The Supplier and SFDC have an existing Salesforce Reseller Agreement executed by the Supplier on 21 March 2019, and have executed an addendum to that agreement in respect of the Resold Subscriptions (the “**Reseller Agreement**”).

The Resold Subscriptions are deemed to be “Services” under the MSA with SFDC, even though Resold Subscriptions are sold by the Supplier to the Customer under this Order Form. As the Customer has direct enforcement rights against SFDC under the MSA and has accepted the terms in the MSA, the following terms and conditions apply to the Resold Subscriptions in lieu of and to the exclusion of the Call Off Terms and the Order Form with the exception of this Annex A.

1. The Customer acknowledges and agrees that any defect, failure, cause of action, breach of warranty, breach or liability under the Order Form arising out of or in connection with the Resold Subscriptions shall be dealt with exclusively under the MSA with SFDC and the Supplier accepts no responsibility for the Resold Subscriptions. Any claims that Customer has against Supplier and/or SFDC with respect to the Resold Subscriptions will be made directly against SFDC under the MSA. Notwithstanding the foregoing, the Supplier acknowledges that it is acting as a collection agent with regard to any service credits which accrue against SFDC and are due to Customer.
2. As the Customer and SFDC have entered into an MSA, SFDC has provided the Supplier with no warranties in respect of the Resold Subscriptions. Therefore, the Supplier provides no warranties, representations or undertakings in respect of the Resold Subscriptions, and disclaims all implied warranties of any kind, whether express, implied or otherwise.
3. In addition to the rights and restrictions set out in the MSA on Customer’s use of the Resold Subscriptions, Customer’s use of the Resold Subscriptions will be subject to additional project special terms required by SFDC as set forth in the Salesforce Order Forms attached below (such additional terms the “**Product Special Terms**”).
4. Not Used.
5. The licence terms in respect of the Resold Subscriptions shall be as set out in the MSA and any claims alleging that any Resold Subscription infringes or misappropriates any third party’s intellectual property shall be exclusively addressed and dealt with between the Customer and SFDC pursuant to the MSA.
6. The Customer agrees that it will (a) be responsible for Users’ compliance with the MSA, Documentation and SFDC Order Forms, (b) use commercially reasonable efforts to prevent



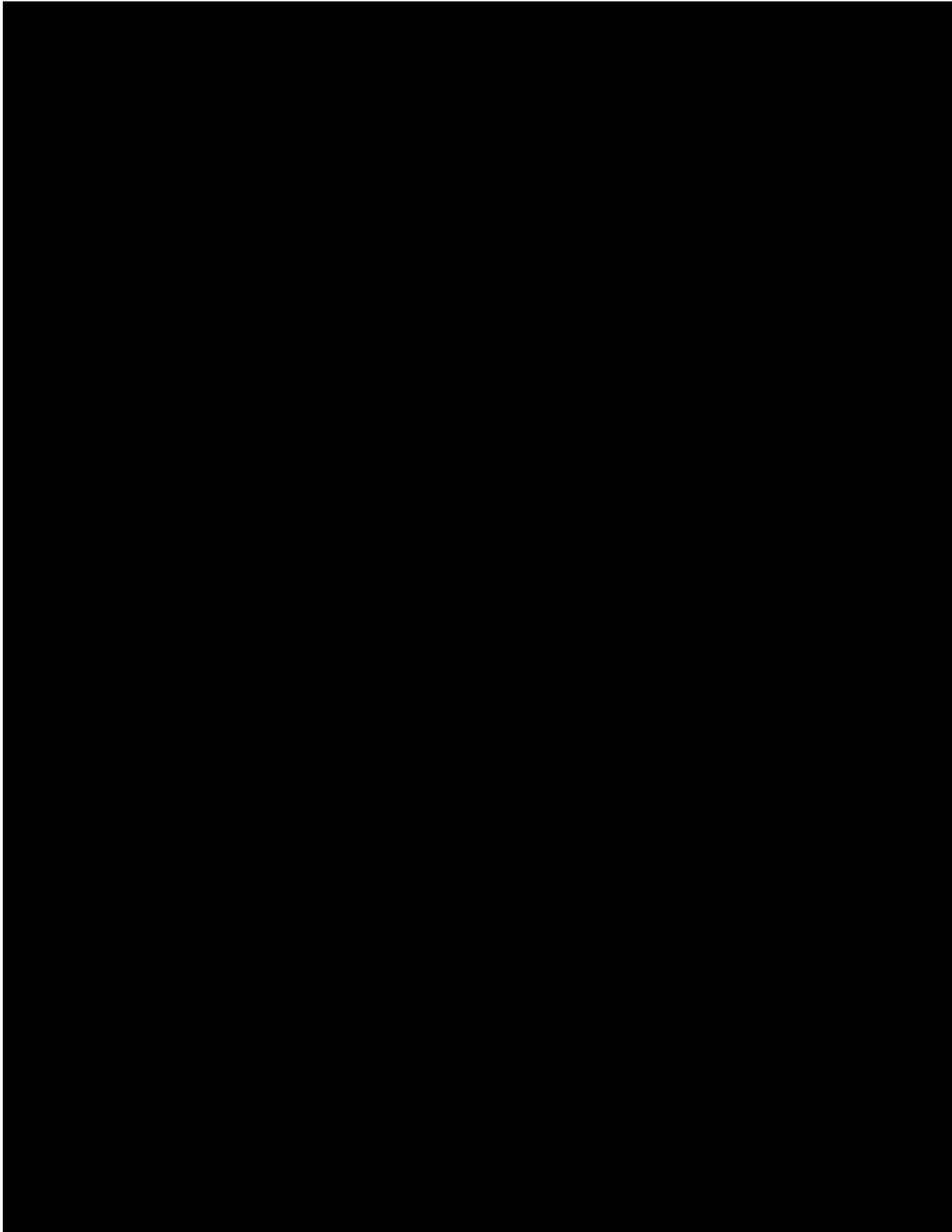
unauthorized access to or use of Resold Subscriptions and associated content, and notify Reseller promptly of any such unauthorised access or use, and (d) use Resold Subscriptions Services and Content only in accordance with the MSA, its Documentation, the Acceptable Use and External Facing Services Policy at <https://www.salesforce.com/company/legal/agreements.jsp>, SFDC Order Forms and applicable laws and government regulations. Any use of the Resold Subscriptions in breach of the foregoing by Customer or Users that in SFDC's judgment threatens the security, integrity or availability of SFDC's services, may result in SFDC's immediate suspension of the Resold Subscriptions. In the event SFDC exercises its rights to suspend in these circumstances, then the Customer acknowledges that the Supplier will not be able to provide the Resold Subscriptions and will not be liable for any losses caused by such suspension.

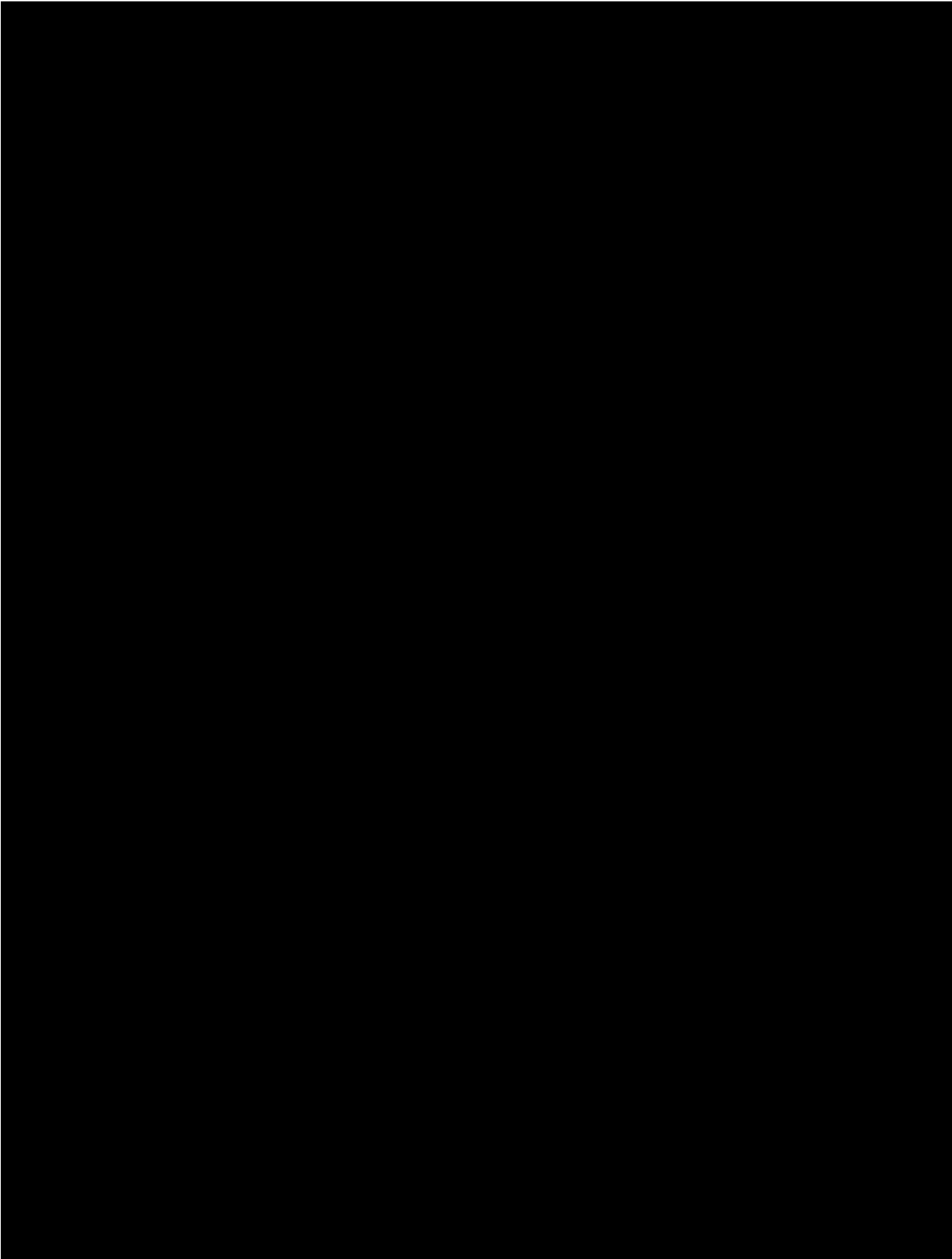
7. In respect of the Resold Subscriptions, the Parties agree that where any Personal Data, as defined in the DPA, is processed by the Supplier or SFDC, the data processing terms and technical and organisational measures set out in Exhibit A (Data Processing Addendum) of the MSA shall apply and are hereby incorporated by reference.
8. In addition to any termination or suspension rights set forth in the Order Form and/or MSA, Customer's use of the Resold Subscriptions may be immediately terminated and/or suspended by the Supplier at SFDC's option, upon notice, where the Customer has not made payments in respect of the Resold Subscriptions in accordance with these terms and that has led to a failure by the Supplier to make its corresponding payment obligations to SFDC with respect to the Resold Subscriptions. To this end, Customer obligation to make payments in full and when due to Supplier with respect to the Resold Subscriptions becomes absolute and unconditional regardless of any on-going dispute between Customer and SFDC under or in connection with the MSA.
9. In the event of termination or expiration of the Order Form for any reason, the Supplier shall use reasonable endeavours to procure that any remaining term in the Resold Subscriptions outstanding at the time of such termination or expiration ("**Legacy Subscriptions**") shall remain in effect until the end of its applicable subscription term, provided that the Customer is not in breach of the MSA and all payments due in connection with such Legacy Subscriptions have been made. Except as provided herein, following a termination or expiration of Order Form, the Supplier is under no obligation to provide the Resold Subscriptions directly to Customer.
10. Notwithstanding anything to the contrary in the Order Form, in no case would any suspension or termination of the Services and/or Resold Subscriptions allow Customer to receive a refund or other compensation from the Supplier relating to the Resold Subscriptions, as payments for the same are made in advance and non-cancellable.
 - a. Refunds in respect of fees for Resold Subscriptions shall only apply where and to the extent SFDC is obligated to refund prepaid fees for Resold Subscriptions, and limited to fees paid by the Supplier in respect of the Resold Subscriptions, who will in turn process the refund under this Order Form.
11. Any amendments to the MSA which have an impact on the Call Off Contract will be promptly notified to the Supplier by the Customer in writing and be subject to a Variation. Conversely

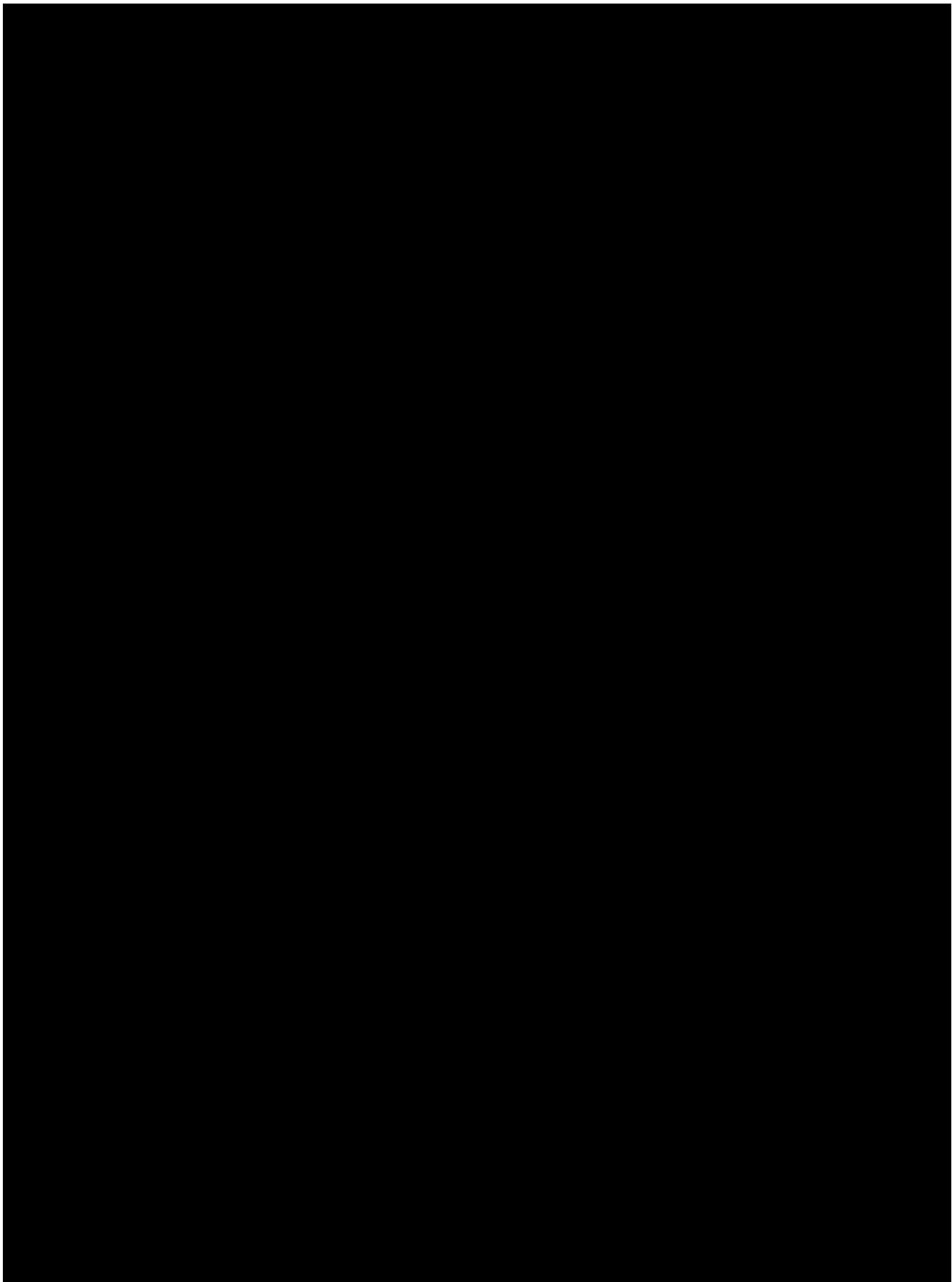


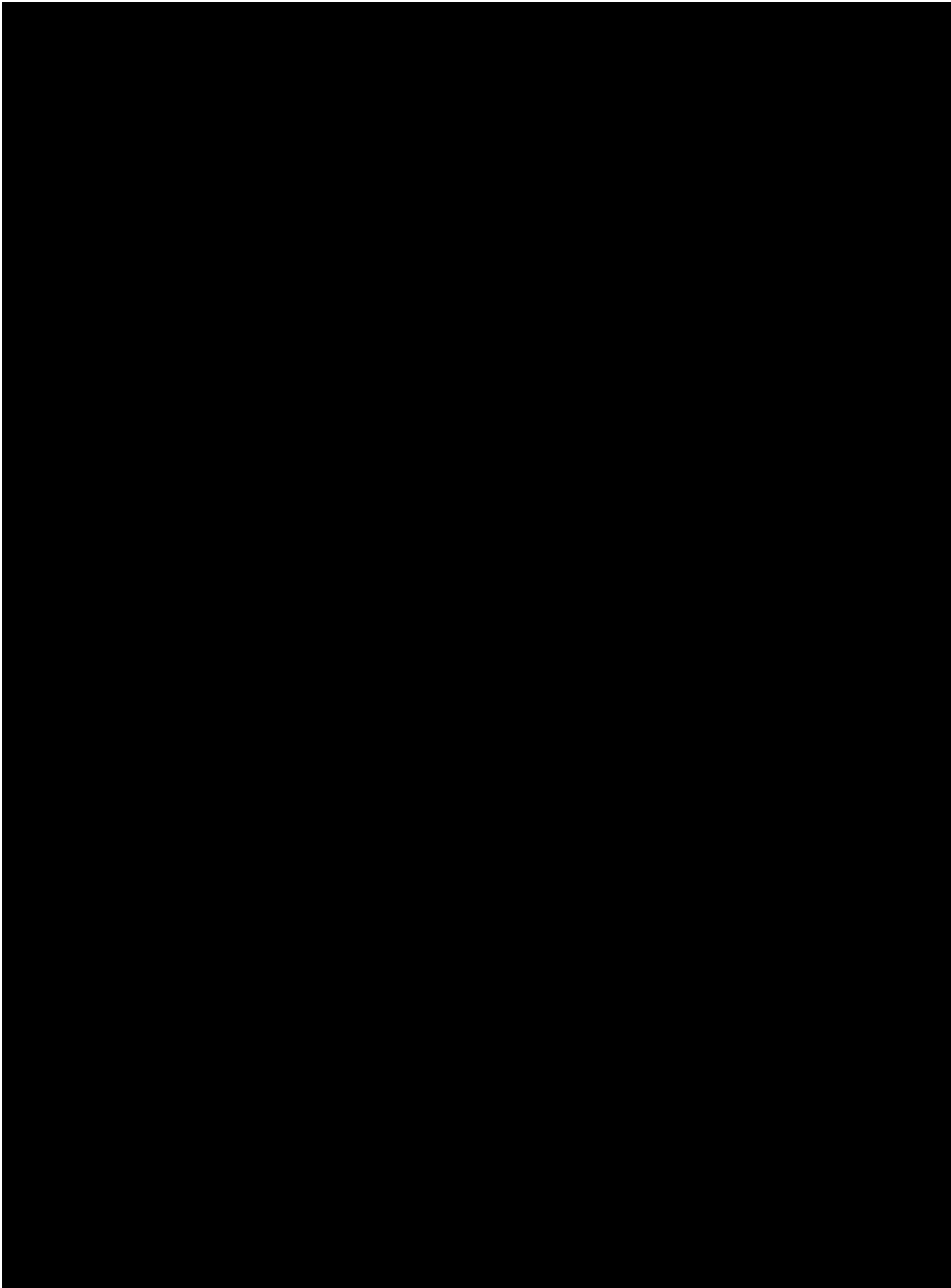
Crown
Commercial
Service

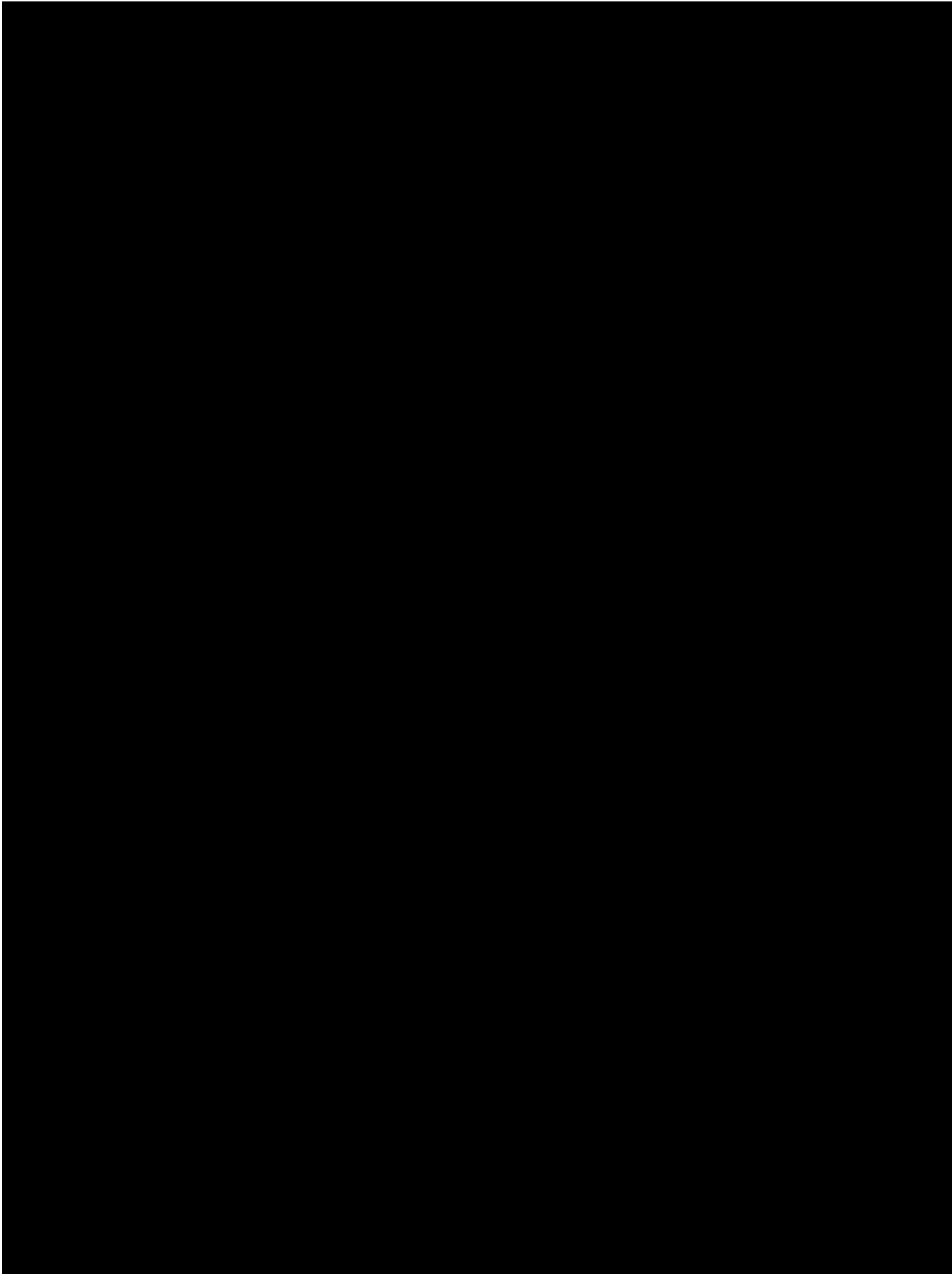
any amendments to the Reseller Agreement which have an impact on the Call Off Contract will be promptly notified to the Customer by the Supplier in writing and be subject to a Variation.

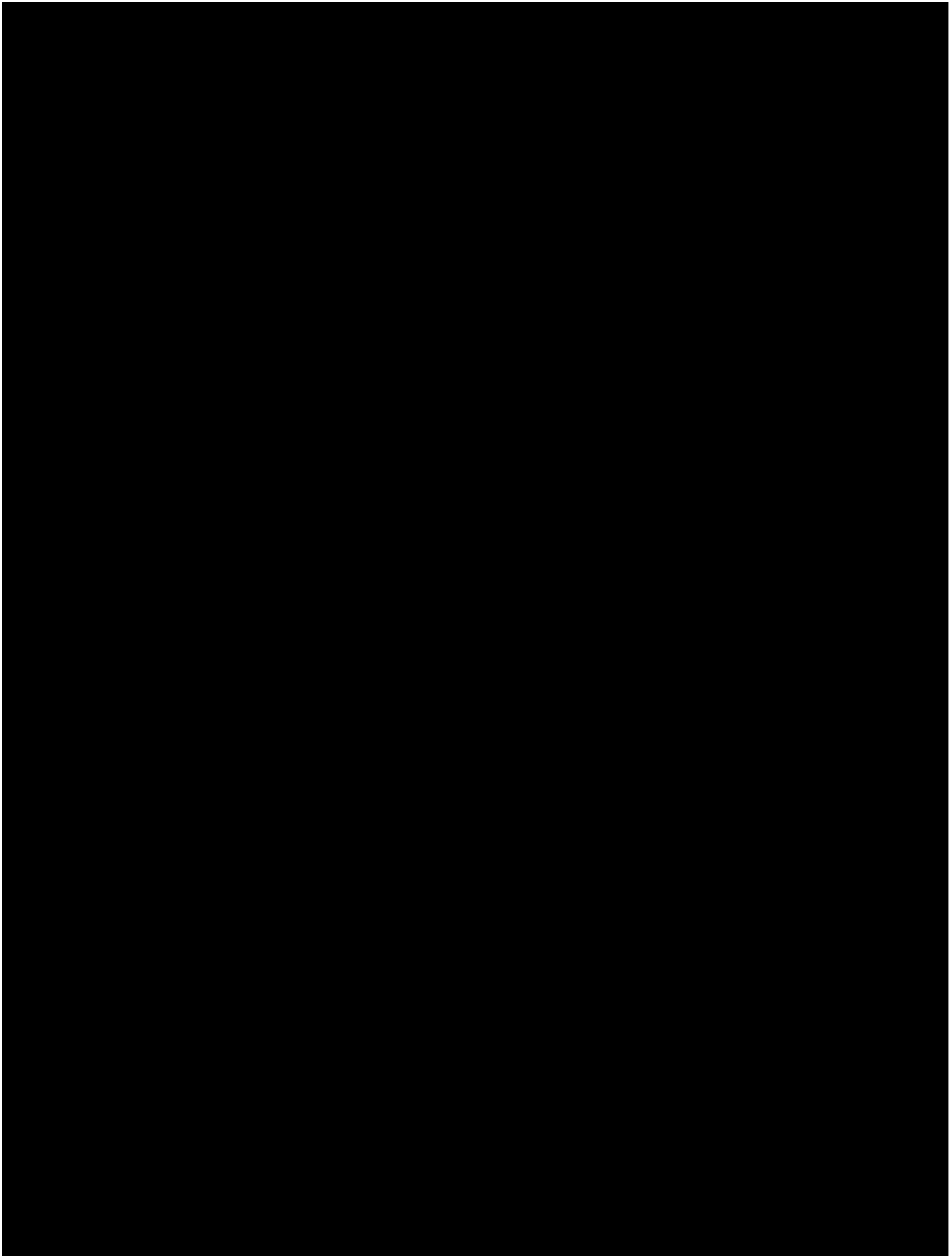


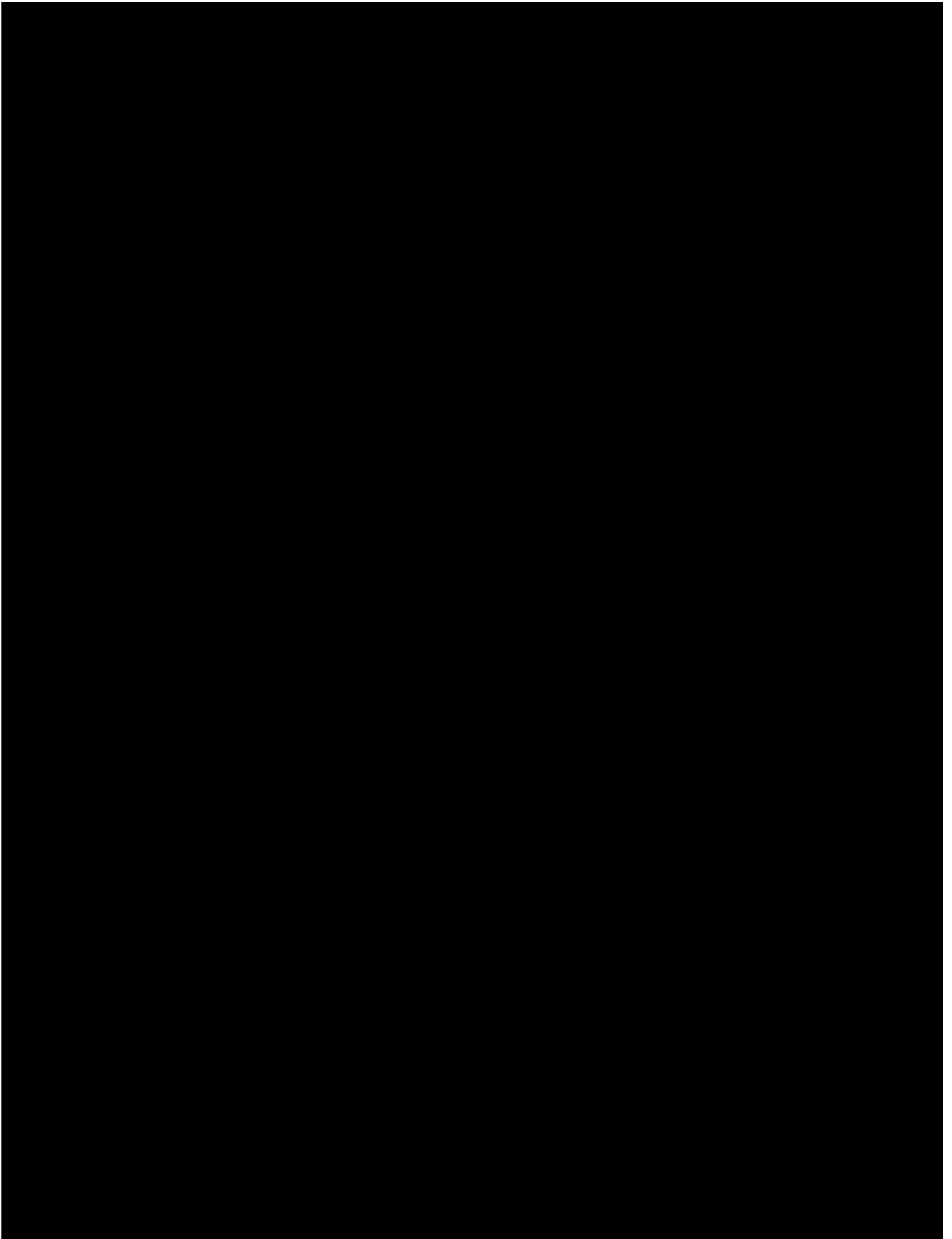


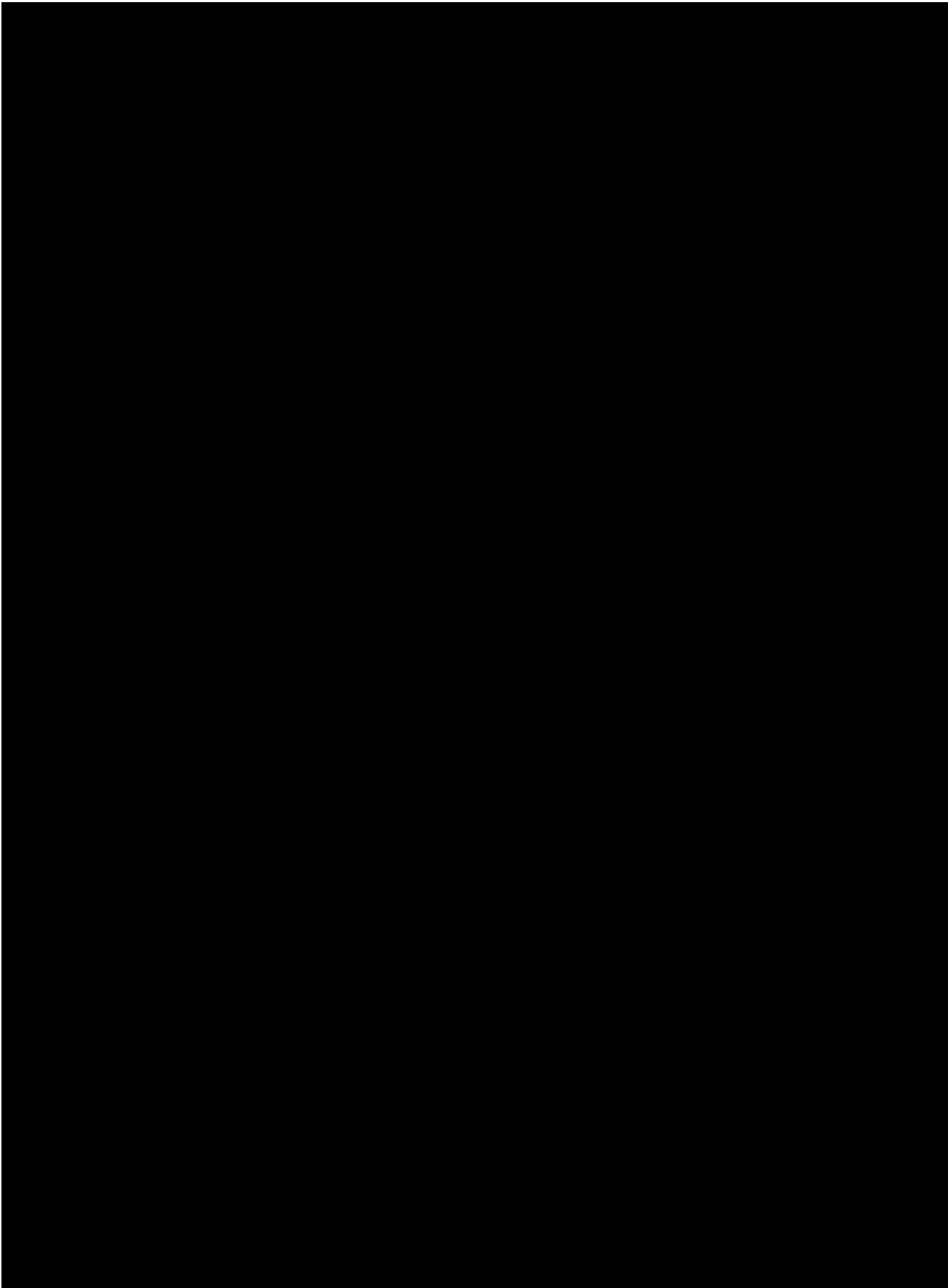


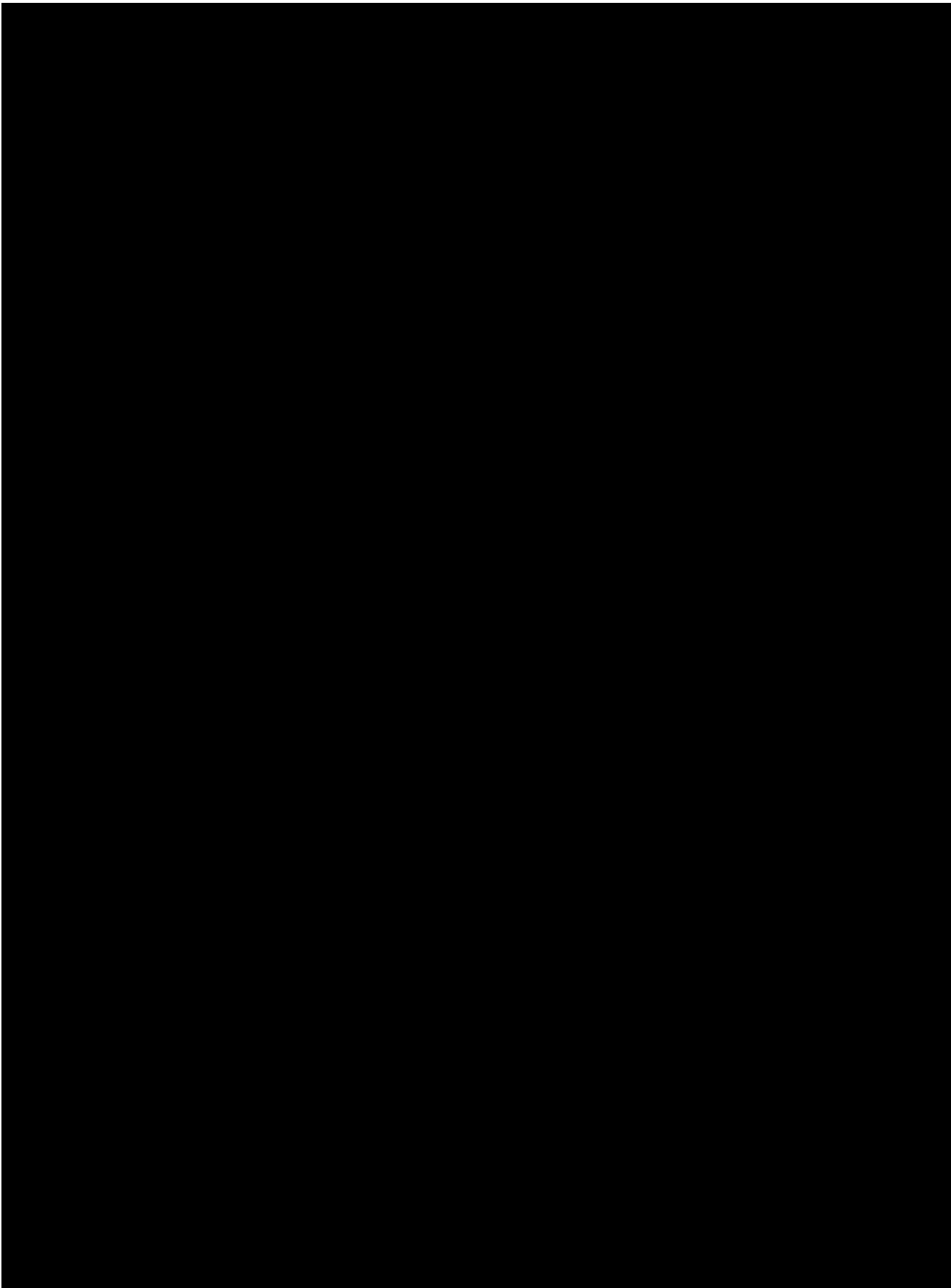






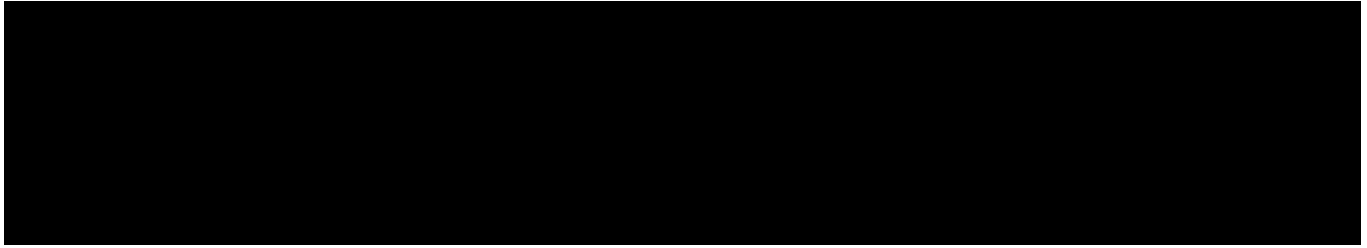


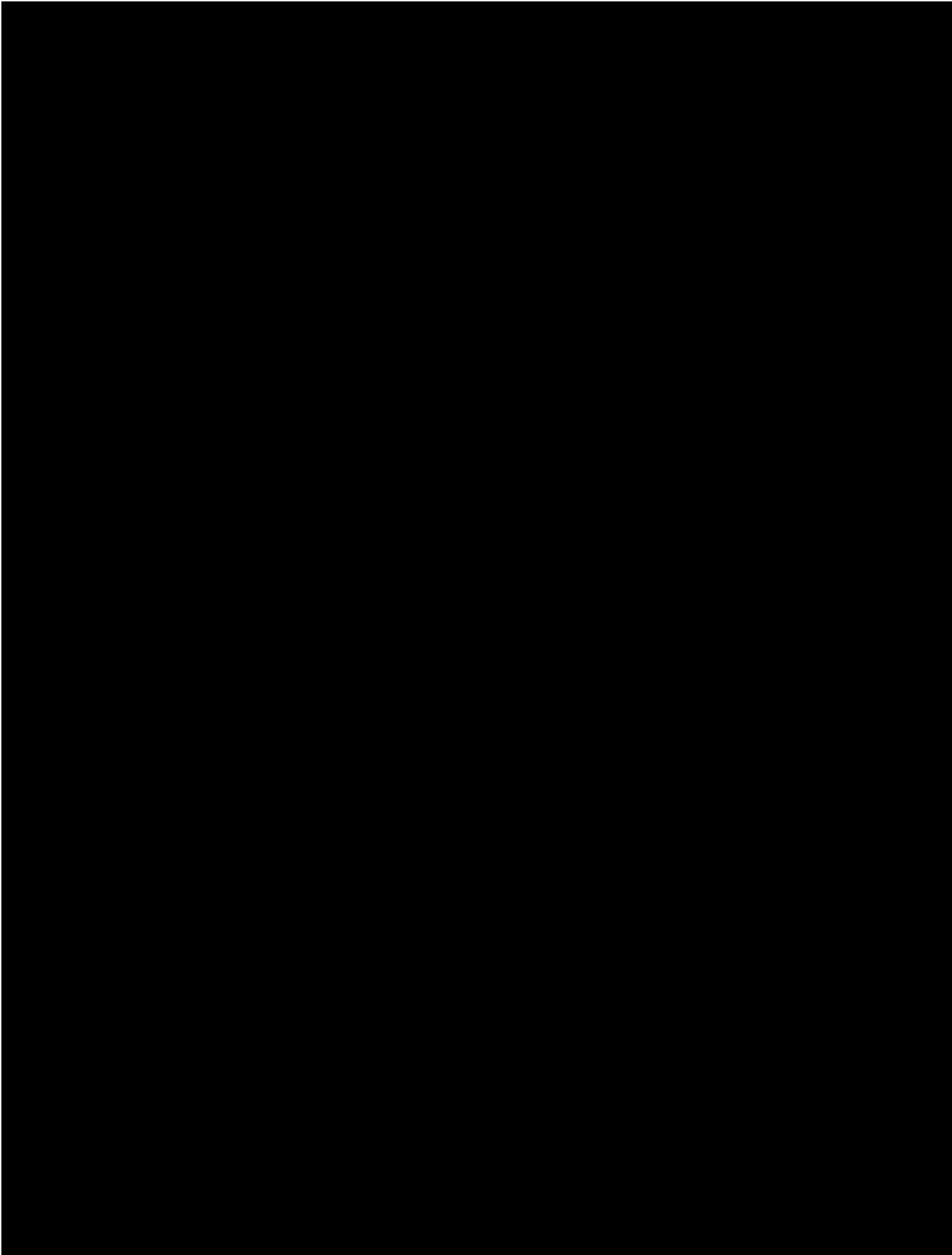


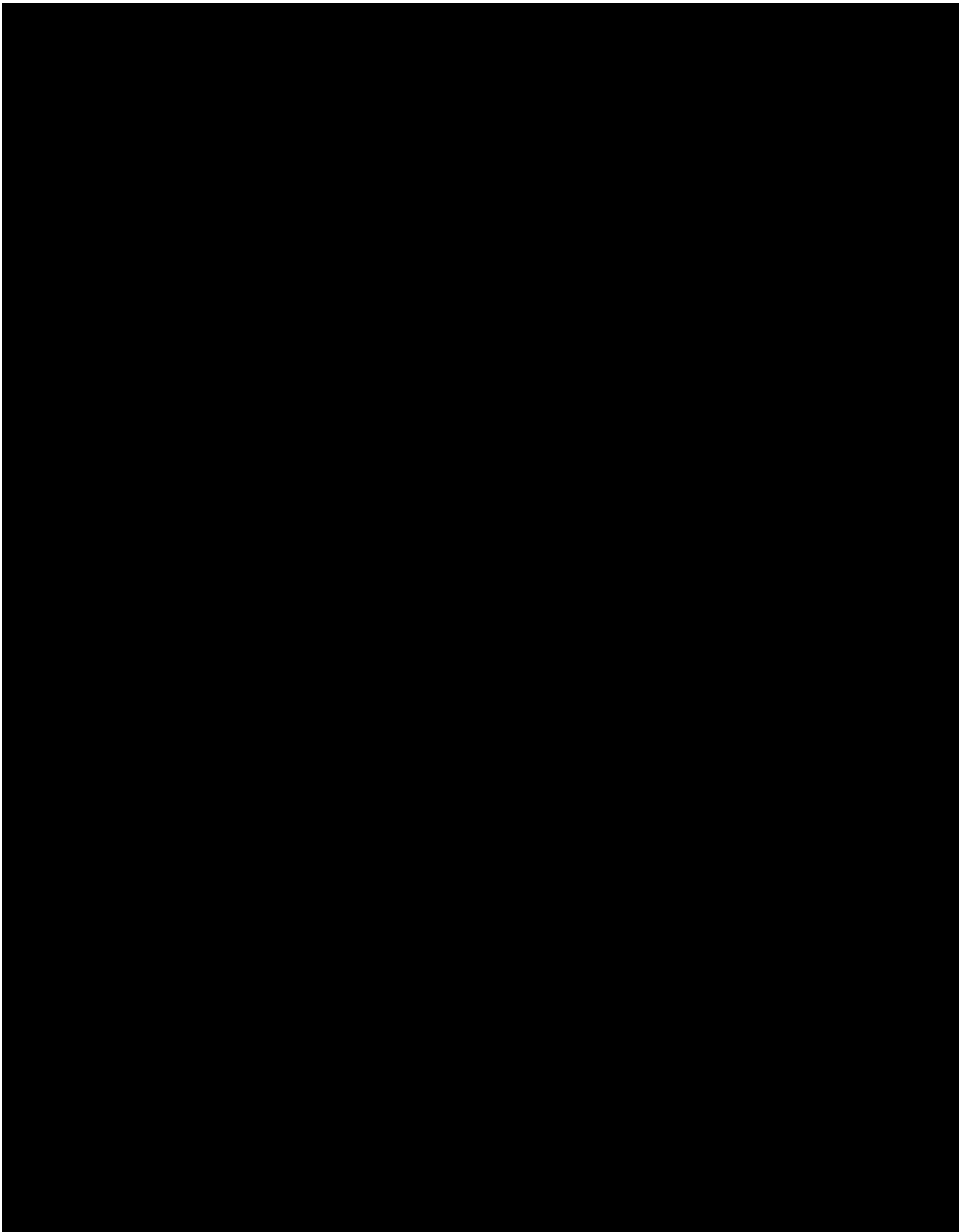


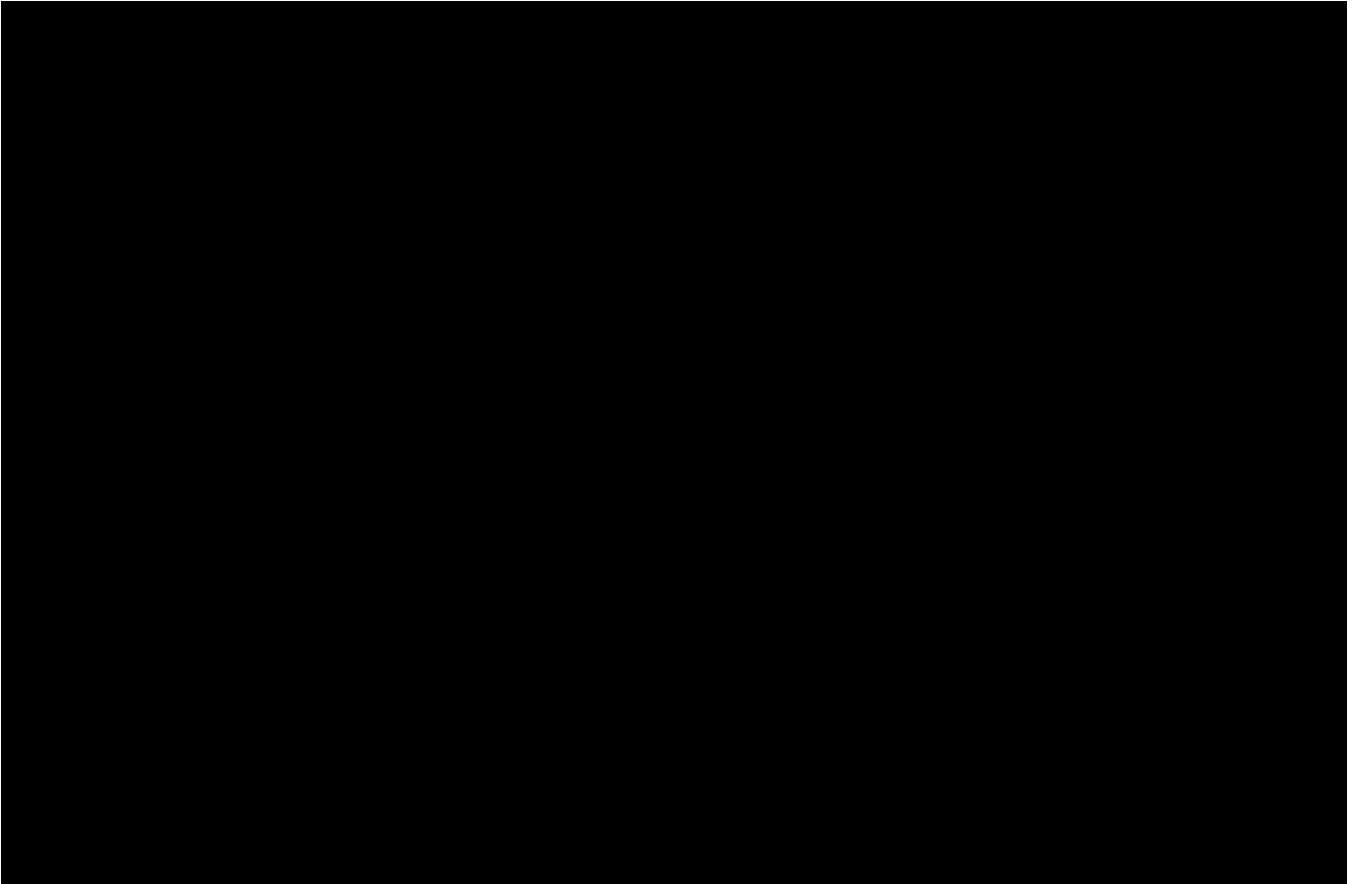


Crown
Commercial
Service











Annex B

Additional Terms to Customer in respect of OwnBackup Services

1. OWNBACKUP SERVICE.

This Annex governs the provision, access to and usage of Internet-based software services specified in this Order Form, including, without limitation their user interfaces, features and functions (collectively **OwnBackup Services**), by the Customer.

2. USE OF OWNBACKUP SERVICE.

- a. **Supplier Responsibilities.** Supplier (i) will keep its passwords secure and confidential and use industry-standard password management practices; (ii) is primarily responsible for Customer Data and all activity in its Ownbackup Services accounts; (iii) will use commercially reasonable efforts to prevent unauthorized access to its account and notify OwnBackup promptly of any such unauthorized access; and (iv) may use the Ownbackup Services only in accordance with the Ownbackup Services' technical documentation and applicable law.
- b. **OwnBackup Support.** OwnBackup will provide support for the Ownbackup Services under the terms of OwnBackup's Customer Support Policy (**Support**), located at <http://www.ownbackup.com/support>.

3. OWNBACKUP PROPERTY.

- a. **Restrictions.** Customer may not (i) sell, resell, rent or lease the Ownbackup Services or use them in a service provider capacity, (ii) use the Ownbackup Services to store or transmit infringing, unsolicited marketing emails, libelous, unlawful or tortious material, or to store or transmit material in violation of third-party rights, (iii) interfere with or disrupt the integrity or performance of the Ownbackup Services, (iv) attempt to gain unauthorized access to the Ownbackup Services or their related systems or networks, (v) reverse engineer or decompile the Ownbackup Services except as otherwise required by law, or (vi) access the Ownbackup Services to build a competitive service or product, or copy any feature, function or graphic for competitive purposes. OwnBackup may suspend the Ownbackup Services to Customer if OwnBackup believes in good faith that Customer's use of the Ownbackup Services poses an imminent threat to the security, availability or legality of the Ownbackup Services; in such event, OwnBackup will work with Customer to address the issue and restore Ownbackup Services as quickly as possible.