SCHEDULE 2.3 - STANDARDS

1 DEFINITIONS

1.1 This Schedule 2.3 (*Standards*) sets out standards, policies and guidelines (together the "**Standards**") that the Supplier shall comply with at all times.

1.2 In this Schedule 2.3 (*Standards*), the following definitions shall apply:

Director-Specific Legislation means the Director specific legislation as set out in Annex 3 to this Schedule 2.3 (*Standards*) and as applicable or notified to the Supplier from time to time.

Director Standards means the policy and guidelines imposed by the Director with which the Supplier is obliged to comply under this Agreement, as set out in Annex 1 to this Schedule 2.3 (*Standards*) and as notified to the Supplier from time to time.

Evergreen means ongoing IT design capability ensuring that the Services continuously evolve to keep up with changing technical standards and innovation.

General Standards means the publicly available standards and guidelines (or equivalent) as set out in Annex 2 to this Schedule 2.3 (*Standards*) and as notified to the Supplier from time to time.

Standards means the Director Standards, the General Standards and the Director-Specific Legislation.

Standards Hub means the Government's open and transparent standards adoption process as documented at http://standards.data.gov.uk/.

Suggested Challenge means a submission to suggest the adoption of new or emergent standards in the format specified on Standards Hub.

2 GENERAL

2.1 Throughout the term of this Agreement, the Parties shall monitor and notify each other of any new or emergent standards which could affect the Supplier's provision, or the Director's receipt, of the Services.

2.2 The Director may request adherence to additional or replacement Standards, in the provision of the Services and the Supplier shall adhere to such additional or replacement Standards in providing the Services.

2.3 Any changes to the Standards, including the adoption of any such new or emergent standard, shall be agreed between the parties through the Change Control Procedure. Notwithstanding this, it shall be the Supplier's responsibility to ensure that its solutions provide ongoing Evergreen capability and that they deliver the Services in accordance with Good Industry Practice at no additional cost to the Director.

2.4 Where this Schedule 2.3 (*Standards*) requires adherence, accreditation or certification to a particular Standard, the Supplier shall ensure it is and remains throughout the Term certified to the Standards required in order to provide the Services. The Supplier shall keep all necessary records and documentation to be able to demonstrate such compliance. The Supplier shall, on each anniversary of the Operational Service Commencement Date or such other date as the Director may reasonably require, demonstrate to the Director's reasonable satisfaction, including by reference to the Supplier's internal assurance processes and through the provisions of Paragraph 6 (*Auditing Compliance*), that the Supplier adheres or remains accredited or certified to the relevant Standard and meets the requirements of the relevant accreditation body or organisation.

2.5 The Supplier's obligation to comply with the Standards pursuant to this Schedule 2.3 (*Standards*) applies notwithstanding the Supplier's general obligation to comply with all applicable Laws, the

provisions allocating responsibility for Change in Law and the obligations in relation to continuous improvement as set out in the Director's Requirements and Schedule 8.8 (*Continuous Improvement*) and, unless otherwise stated in this Schedule 2.3 (*Standards*), shall apply from the Effective Date and at all times during the Term.

2.6 Where one or more conflicting Standards apply to a particular situation, the Director shall determine at the Director's sole discretion which Standard shall apply and the Supplier shall comply with the Director's instructions.

2.7 Where any conflict occurs between one or more Standards and the Service Description, the Director shall determine at its sole discretion which shall take priority.

2.8 The Supplier shall bear all costs relating to any planned or anticipated changes in Standards as at the Effective Date.

2.9 The Supplier shall neither be relieved of its obligations to supply the Services in accordance with this Agreement nor be entitled to an increase in the Charges as the result of any changes to, replacement of or the introduction of additional Standards which might be known to, or reasonably capable of being anticipated by a service provider acting in accordance with Good Industry Practice.

2.10 Any increase in the Charges, or relief from the Supplier's obligations, where the provisions of Paragraph 2.5 of this Schedule 2.3 (*Standards*)do not apply, shall be implemented in accordance with the Change Control Procedure, provided that the Supplier shall bear the first one hundred thousand pounds (£100,000) in respect of all such Changes in each Contract Year.

2.11 Where a new or emergent standard is to be developed or introduced, the Supplier shall work with the Director, including cooperating with any Relevant Third Party Suppliers and compliance with the obligations set out in the Collaboration Agreement in relation to such new or emergent Standards on identifying the impact of such proposal on:

2.11.1 the Supplier's provision of the Services;

2.11.2 the Director's receipt of the Services; and

2.11.3 the Relevant Third Party Suppliers provision of any Related Services.

3 DIRECTOR POLICIES AND GUIDELINES

3.1 The Supplier shall comply with the Director's policies and guidelines listed in Annex 1 at all times in providing the Services.

3.2 If the Supplier reasonably believes that the Director's policies and guidelines are not applicable to the Supplier, the Supplier shall notify the Director and comply with the Director's instructions in respect of such policies and guidelines.

3.3 If the Supplier reasonably believes it is incapable of complying with such policies and guidelines or that they are written in a manner that does not enable the Supplier to full comply with them, the Supplier shall notify the Director and shall agree with the Director any modifications to the polices and guidelines and/or the Services as may be required. Before any such amendments are made, the Director may require the Supplier to undertake an Impact Assessment in respect of the impact of such amendments on the elements referred to in Paragraph 2.11.

3.4 Where the Supplier believes that a Supplier's policy or guidelines is equivalent to a Director's policy or guideline then, subject to the Supplier demonstrating to the Director that such policy or guideline is equivalent then, at the Director's discretion, the Supplier may substitute the Director's policy or guideline with the Supplier's policy or guidelines.

4 PUBLICLY AVAILABLE STANDARDS AND POLICIES

The Supplier shall as a minimum adhere to the Standards listed in Annex 2 (or those equivalent Standards as agreed with or determined by the Director) at all times in providing the Services.

5 DIRECTOR-SPECIFIC LEGISLATION

5.1 Without prejudice to the Supplier's obligations under Clause 5.3 of the Agreement to deliver the Services in accordance with all applicable Laws the Supplier shall comply with and shall provide the Services in such manner as to enable the Supplier to comply with any Laws specifically relating to the Director including but not limited to those listed in Annex 3.

5.2 For the avoidance of doubt, the costs for compliance with any Change in Law shall be as stated in accordance with Clause 13 of the Agreement and the costs of implementing such change shall not, unless otherwise agreed by the Director, be included within the Charges allowance pursuant to Paragraph 2.10 above.

6 AUDITING COMPLIANCE

6.1 In addition to the general obligation to demonstrate compliance under Paragraph 2.4, the Supplier shall commission an independent annual audit in respect of its compliance with this Schedule 2.3 (*Standards*), the cost of such audit to be borne by the Supplier.

6.2 Prior to commissioning the audit, the Supplier shall engage with the Director to agree the scope of the audit, which must be approved in writing by the Director but which shall include as a minimum the requirement to review compliance with the certification as required under this Schedule 2.3 (*Standards*).

6.3 The Supplier shall ensure the Director has unfettered access to the resultant audit reports and the auditor for the purpose of understanding such audit reports.

6.4 If an audit undertaken pursuant to this Schedule 2.3 (*Standards*) identifies that the Supplier has committed a Default, this shall constitute a Notifiable Default.

ANNEX 1 – DIRECTOR'S POLICIES AND GUIDANCE

Director's Policies and Guidelines *Entries with an asterisk (*) are in development by the Director.*
NS&I Business Continuity Management Policy v1.0
NS&I Information and Data Handling Policy v1.0
NS&I Security Vetting Policy v1.5
NS&I Physical Security Policy v2.1
NS&I Risk Management Framework v2.7
NS&I Offshoring of Information Assets Policy v1.4
NS&I Password Protection Policy v1.8
NS&I Acceptable Use Policy v2.7
[NS&I Backup and Restore Policy*]
NS&I Brand Guidelines v5
NS&I's Customer Accessibility Policy v1.1
NS&I Enterprise Data Strategy v1.0
NS&I Enterprise Architecture Principles v2.1
[NS&I IT Service Continuity Management Policies and Procedures*]
[NS&I Availability Management Policies and Procedures*]
[NS&I Capacity Management Policies and Procedures*]
[NS&I Service Asset and Configuration Management Policies and Procedures*]
NS&I Customer Due Diligence Policy v1.3
NS&I Complaints Handling Policy v14 Framework
NS&I Compensation and Goodwill Policy v8
NS&I Content Strategy and Blueprint v1.3
NS&I Data Quality Management Approach v1.0
NS&I Access Control Policy v1.1
NS&I Cloud Security Standard v1.0 (and NS&I Cloud Security Standard Exception Request Form v1.0)
NS&I Configuration Management Policy v1.0
NS&I Identification and Authentication Policy v1.1
NS&I Incident Response Policy v1.2
NS&I Information System Media Protection Policy v1.1
NS&I Maintenance Policy v1.1
NS&I Mobile Device Policy v3.1
NS&I Security and Awareness Training Policy v1.1
NS&I Security Assessment and Authorisation Policy v1.1
NS&I Security Supplier Management Policy v1.0
NS&I System and Information Integrity Policy v1.1

NS&I System and Services Acquisition Policy v1.1
NS&I Systems and Communication Policy v1.1
Customer Data Retention Rules (CDDR) v8.5
Financial Promotions and Customer Communications Manual v2.1
NS&I Security Classifications Policy V1.0
NS&I Cyber Security Strategy V1.0
NS&I Information and Data Handling Policy and Standard V1.0
NS&I Information Security Policy V1.0

Note; those Standards designated in the above table by square brackets and an asterisk have not been received by the Supplier at the Effective Date and shall be considered to be a new Standard for the purpose of Paragraph 2.3 of this Schedule 2.3 (*Standards*).

ANNEX 2 – PUBLICLY AVAILABLE STANDARDS AND POLICIES

Publicly Available Standards and Policies	Level of Compliance Required (Adherence/Accreditation/Assurance)
The Supplier shall (when designing, implementing and delivering the Services) adopt the applicable elements of HM Government's Technology Code of Practice as documented at https://www.gov.uk/service-manual/technology/code-of-practice.html.	Adherence
Government Functional Standard GovS 005	Adherence
ISO/IEC 27031:2011 *Guidelines for information and communication technology readiness for business continuity*	Adherence
Government Social Value Model as currently contained at https://www.gov.uk/government/publications/procurement-policy-note-0620-taking-account-of-social-value-in-the-award-of-central-government-contracts	Adherence
Her Majesty's Treasury Orange Book – Management of Risk, Principles and Concepts	Adherence
NS&I Information Asset Framework	Adherence
HMG Security Policy Framework (SPF)	Adherence
ISO 9001:2008 Quality Management	Accreditation
IS0 14001: Environmental Management	Accreditation
ISO/IEC 20000-1 2018 "Information technology — Service management – Part 1"	Adherence
ISO/IEC 20000-2 2019 "Information technology — Service management – Part 2"	Adherence
ISO27001: 2013 Information Security Standard	Accreditation
ISO 10007: 2017 "Quality management systems – Guidelines for configuration management"	Adherence
ISO 22313:2020 "Security and resilience. Business continuity management systems. Guidance on the use of ISO 22301" and, ISO/IEC 27031:2011 and ISO 22301:2019	Assurance
ISO 20022	Assurance
ISO22301 2019	Accreditation
NCSC Cloud Security Guidance	Assurance
Government Functional Standard GovS 007	Adherence

Publicly Available Standards and Policies	Level of Compliance Required (Adherence/Accreditation/Assurance)
Information Technology Information Library (ITIL) (Version 4) For the purposes of management of the Services and delivery performance the Supplier shall make use of Software that complies with Good Industry Practice including availability, change, incident, knowledge, problem, release & deployment, request fulfilment, service asset and configuration, service catalogue, service level and service portfolio management. If such Software has been assessed under the ITIL Software Scheme as being compliant to "Bronze Level", then this shall be deemed acceptable.	Adherence
ISO 45001 – Health and Safety Management System	Accreditation
Open Web Application Security Projects (OWASP): including "Top ten vulnerabilities"	Adherence *Evidence of Adherence shall include documented evidence of:* *- Solution design and development to mitigate the vulnerabilities* *- Independent penetration testing to demonstrate that the vulnerabilities have been mitigated*
The Open Group Architecture Framework (TOGAF) (Version 9)	Adherence
Communications Electronics Security Group (CESG) Good Practices and guidelines	Adherence
Baselines Personnel Security Standard (BPSS)	Adherence
HMG Security Classifications	Adherence
Public Records Act 1958	Adherence
COBIT	Adherence
HMG Cyber Security Standard	Adherence
HMG Physical Security Standard	Adherence
HMG Personnel Security Standard	Adherence
HMG Incident Management Standards	Adherence
European Payments Council (EPC) 153-10: Audit trails in security systems	Adherence
UK Retail banking regulations and guidance	Adherence
BCI Good Practice Guidelines	Adherence
NCSC 10 Steps to Cyber Security	Adherence
NCSC Device Security Guidance (Logging and Protective Monitoring)	Adherence
NCSC Device Security Guidance	Adherence

Publicly Available Standards and Policies	Level of Compliance Required (Adherence/Accreditation/Assurance)
NCSC Design and Build a privately hosted Public Key Infrastructure	Adherence
NCSC Secure Sanitisation of Storage Media	Adherence
NCSC Protecting Bulk Personal Data	Adherence
NCSC Zero Trust Architecture Design Principles	Adherence
NCSC Protective DNS for the Private Sector	Adherence
NCSC Connected Places Cyber Security Principles	Adherence
NCSC Security principles for cross domain solutions	Adherence
Business Continuity Institute (BCI); Good practice and guidelines	Adherence
CyberEssentials Plus	Accreditation
PCI DSS	Adherence
Orange Book	Adherence
All applicable elements of the NIST Cyber Security Framework	Independent review annually to PRISMA level 4

1 OPEN DATA STANDARDS & STANDARDS HUB

1.1 The Supplier shall comply to the extent within its control with UK Government's Open Standards Principles as documented at https://www.gov.uk/government/publications/open-standards-principles/open-standards-principles, as they relate to the specification of Standards for software interoperability, data and document formats in the IT Environment.

1.2 Without prejudice to the generality of Paragraph 2.11, the Supplier shall, when implementing or updating a technical component or part of the Software or Supplier Solution where there is a requirement under this Agreement or opportunity to use a new or emergent Standard, submit a Suggested Challenge compliant with the UK Government's Open Standards Principles (using the process detailed on Standards Hub and documented at http://standards.data.gov.uk/). Each Suggested Challenge submitted by the Supplier shall detail, subject to the security and confidentiality provisions in this Agreement, an illustration of such requirement or opportunity within the IT Environment, Supplier Solution and Government's IT infrastructure and the suggested open standard.

1.3 The Supplier shall ensure that all documentation published on behalf of the Director pursuant to this Agreement is provided in a non-proprietary format (such as PDF or Open Document Format (ISO 26300 or equivalent)) as well as any native file format documentation in accordance with the obligation under Paragraph 1.1 of this Annex 2 to comply with the UK Government's Open Standards Principles, unless the Director otherwise agrees in writing.

2 ACCESSIBLE STANDARDS

2.1 The Supplier shall comply with (or with equivalents to):

2.1.1 the World Wide Web Consortium (W3C) Web Accessibility Initiative (WAI) Web Content Accessibility Guidelines (WCAG) 2.1 Conformance Level AA;

2.1.2 ISO/IEC 13066-1: 2011 Information Technology – Interoperability with assistive technology (AT) – Part 1: Requirements and recommendations for interoperability;

2.1.3 the Public Sector Bodies (Websites and Mobile Applications) (No.2) Accessibility Regulations 2018; and

2.1.4 the Equalities Act (2010).

ANNEX 3 – DIRECTOR-SPECIFIC LEGISLATION

Director-Specific Legislation
National Debt Act 1972
The National Loans Act 1968
National Savings Bank Act 1971
The National Savings Regulations 2015
The National Savings Regulations No.2 Regulations 2015

SCHEDULE 2.4 - SECURITY MANAGEMENT

SECURITY ASSURANCE

1 Definitions

1.1 In this Schedule 2.4 (*Security Management*):

Anti-Malicious Solution means a solution that scans for, prevents the introduction of, identifies and contains the spread and impact of possible Malicious Software in the IT Environment.

Breach of Security means an event that results, or could result, in:

(a) any unauthorised access to or use of the Director Data, the Services and/or the Information Management System; and/or

(b) the loss, corruption and/or unauthorised disclosure of any information or data (including the Confidential Information and the Director Data), including any copies of such information or data, used by the Director and/or the Supplier in connection with this Agreement.

Bulk Customer Data means a data set relating to Customers that contains at least one thousand (1,000) Customer records and that allows individuals to be directly identified.

Central Security Monitoring Service means the overarching monitoring and incident response service provided on behalf of the Director by a nominated Relevant Third Party Supplier across the Information Management System.

Certification Requirements means the information security requirements set out in Paragraph 8.

CHECK Service Provider means a company which has been certified by the National Cyber Security Centre, holds "Green Light" status and is authorised to provide the IT Health Check services required by Paragraph 9.1.

Core Information Management System means those information assets, IT systems and/or Sites which will be used by the Supplier and/or its Sub-contractors to Process Director Data, together with the associated Information Management System (including organisational structure, controls, policies, practices, procedures, processes and resources) which the Director has determined in accordance with Paragraph 4.2 shall be subject to the provisions of this Schedule.

CREST Service Provider means a company with a SOC Accreditation from CREST International.

Cyber Essentials means the Cyber Essentials certificate issued under the Cyber Essentials Scheme.

Cyber Essentials Plus means the Cyber Essentials Plus certificate issued under the Cyber Essentials Scheme.

Cyber Essentials Scheme means the Cyber Essentials scheme operated by the National Cyber Security Centre.

Enhanced Privileges means greater access rights to the Information Management System for administration purposes which provides individuals, such as system and database administrators, with the ability to make changes to the Information Management System, which Supplier Personnel without such privileges are prohibited from.

Information Management System means the Core Information Management System and the Wider Information Management System.

Information Security Approval Statement means a notice issued by the Director which sets out the information risks which the Supplier has identified as being associated with using the Core Information Management System and confirms that:

(a) the Director is satisfied that all relevant risks have been identified, adequately and appropriately addressed by the Supplier;

(b) the Director has accepted any residual risks; and

(c) the Supplier may use the Core Information Management System to Process Director Data.

Information Security Assurance Assessment means the set of policies, standards, guidelines, procedures, systems and processes which the Supplier shall implement, maintain and update in accordance with Paragraph 6 in order to manage, mitigate and, where possible, avoid information security risks including cyber-attacks, hacks, data leaks, Personal Data Breaches and/or theft and which shall be prepared by the Supplier using the template set out in Annex 3**.**

Integration Platform means the integration platform sitting at the centre of the architecture, providing a bridge between all platforms and providing foundation connectivity, routing and security capabilities, provided by or on behalf of the Director by a Relevant Third Party Supplier.

IT Health Check has the meaning given in Paragraph 9.1.

Personal Data Processing Statement means a document setting out:

(a) the types of Personal Data which the Supplier and/or its Sub-contractors Processes or will Process under this Agreement;

(b) the categories of Data Subjects whose Personal Data the Supplier and/or its Sub-contractors Processes or will Process under this Agreement;

(c) the nature and purpose of such Processing;

(d) the locations at which the Supplier and/or its Sub-contractors Process Personal Data under this Agreement; and

(e) the Protective Measures that the Supplier and, where applicable, its Sub-contractors have implemented to protect Personal Data Processed under this Agreement against a Breach of Security (insofar as that Breach of Security relates to data) or a Personal Data Breach.

Process means any operation which is performed on data, whether or not by automated means, including collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Red Team, Purple Team Testing means cyber security testing strategies, including penetration testing, as recognised within the cyber security industry as Good Industry Practice.

Required Changes Register mean the register within the Security Management Plan which is to be maintained and updated by the Supplier and which shall record each of the changes that the Supplier shall make to the Core Information Management System and/or the Security Management Plan as a consequence of the occurrence of any of the events set out in Paragraph 7.2 together with the date by which such change shall be implemented and the date on which such change was implemented.

Risk Register is the risk register within the Information Security Assurance Assessment which is to be prepared and submitted to the Director for approval in accordance with Paragraph 6.

Security Incident Management Process means the process which the Supplier shall implement immediately after it becomes aware of a Breach of Security which is intended to restore normal

operations as quickly as possible, minimising any adverse impact on the Director Data, the Director, the Relevant Third Party Suppliers, the Services and/or users of the Services and which shall be shall be prepared by the Supplier as part of the Security Management Plan.

Security Management Plan means the document prepared by the Supplier using the template in Annex 3, comprising:

(a) the Information Security Assurance Assessment;

(b) the Personal Data Processing Statement;

(c) the Required Changes Register; and

(d) the Security Incident Management Process.

Security Test has the meaning given in Paragraph 9.1.

Special Category Personal Data means the categories of Personal Data set out in article 9(1) of the UK GDPR.

Vulnerability Correction Plan has the meaning given in Paragraph 9.4.1.

Wider Information Management System means those information assets, IT systems and/or Sites which will be used by the Supplier, the Relevant Third Party Supplier or their respective Sub-contractors to Process Authority Data as part of the end to end solution which have not been determined by the Director to form part of the Core Information Management System, together with the associated information management system (including organisational structure, controls, policies, practices, procedures, processes and resources).

2 Introduction

2.1 This Schedule 2.4 (*Security Management*) sets out:

2.1.1 the arrangements the Supplier must implement before, and comply with when, providing the Services and performing its other obligations under this Agreement to ensure the security of the Director Data and the Information Management System;

2.1.2 the Certification Requirements applicable to the Supplier and each of those Sub-contractors which Processes Director Data;

2.1.3 the security requirements in Annex 1, with which the Supplier must comply;

2.1.4 the Security Tests which the Supplier shall conduct on the Core Information Management System during the Term; and

2.1.5 the Supplier's obligations to:

(a) return or destroy Director Data on the expiry or earlier termination of this Agreement;

(b) prevent the introduction of Malicious Software into the Supplier System and to scan for, contain the spread of, and minimise the impact of Malicious Software which is introduced into the Supplier System in Paragraph 11; and

(c) report Breaches of Security to the Director.

2.2 Where there is a reference to the Director's rights or responsibilities in this Schedule 2.4 (*Security Management*), such rights or responsibilities may be exercised by the Director or, if so directed by the Director from time to time, by a Relevant Third Party Supplier who is delivering the Central Security Monitoring Service on behalf of the Director.

3 Principles of Security

3.1 The Supplier acknowledges that the Director places great emphasis on the confidentiality, integrity and availability of the Director Data and, consequently on the security of:

3.1.1 the Sites;

3.1.2 the IT Environment;

3.1.3 the Supplier Personnel;

3.1.4 the Information Management System; and

3.1.5 the Services.

3.2 Notwithstanding the involvement of the Director in assessing the arrangements which the Supplier implements to ensure the security of the Director Data and the Information Management System, the Supplier shall be, and shall remain, responsible for:

3.2.1 the security, confidentiality, integrity and availability of the Director Data whilst that Director Data is under the control of the Supplier or any of its Sub-contractors; and

3.2.2 the security of the Core Information Management System.

3.3 The Supplier shall:

3.3.1 comply with the security requirements in Annex 1; and

3.3.2 ensure that each Sub-contractor that Processes Director Data complies with the Sub-contractor Security Requirements.

3.4 The Supplier shall ensure its leadership's commitment to and support of cyber security, information security and risk management to protect the Director against data exposure. It shall appoint individuals at the relevant level with the relevant skill and experience to discharge their duties under this Agreement, such roles and individuals to be designated as Key Personnel in Schedule 9.2 (*Key Personnel*) as appropriate.

3.5 The Supplier shall provide the Director with access to Supplier Personnel responsible for security and information assurance to facilitate the Director's assessment of the Supplier's compliance with its obligations set out in this Schedule at reasonable times on reasonable notice.

4 Information Management System

4.1 The Information Management System comprises the Core Information Management System and the Wider Information Management System.

4.2 The Director shall be responsible for determining the boundary between the Core Information Management System and the Wider Information Management System. In order to enable the Director to make such determination, the Supplier shall provide the Director with such documentation and information that the Director may reasonably require regarding any information assets, IT systems and/or Sites which will be used by the Supplier or any Sub-contractor to Process Director Data together with the associated information management system (including organisational structure, controls, policies, practices, procedures, processes and resources). The Director shall notify the Supplier, as soon as reasonably practical following the receipt of such documentation and information, of its decision regarding the component parts of the Core Information Management System and its boundary with the Wider Information Management System (noting that, except where explicitly agreed with the Director, the Core Information Management System shall only interact with the Wider Information Management System via the Integration Platform). The Supplier shall reproduce the Director's decision as a diagram documenting the Core Information Management System, the Wider Information

Management system and the boundary between the two. This diagram shall form part of the Security Management Plan.

4.3 Any proposed change to the component parts of the Core Information Management System or the boundary between the Core Information Management System and the Wider Information Management System shall be notified and processed in accordance with the Schedule 8.2 (*Change Control Procedure*).

5 Central Security Monitoring Service

5.1 Notwithstanding the obligations on the Supplier in respect of the Core Information Management System, the Supplier shall also cooperate, collaborate and engage as necessary with the Central Security Monitoring Service and the Relevant Third Party Suppliers in respect of the Central Security Monitoring Service and to fulfil all roles and responsibilities as defined by the Central Security Monitoring Service to ensure a clear approach to the detection and response to any cyber security incidents.

5.2 In its engagement with and obligations in respect the Central Security Monitoring Service the Supplier shall comply with the requirements set out in Schedule 2.1 (*Service Description*), including as a minimum:

5.2.1 comply with the NIST Cyber Security Framework (Level 4) as amended from time to time;

5.2.2 providing the Director and the Central Security Monitoring Service with:

(a) the inventory of physical and virtual devices; and

(b) the inventory of software platforms, applications and external services used to provide the Core Information Management System;

5.2.3 monitoring of all devices and, where relevant, external service providers, within the scope of the Core Information Management System (including those used by Sub-contractors) by and/or in accordance with the instructions of the Central Security Monitoring Service;

5.2.4 immediately communicate any suspected or actual Breach of Security to the Central Security Monitoring Service and the Director and continue to keep all parties informed throughout any incident response and recovery activities;

5.2.5 providing log, event and other incident/vulnerability data to the Central Security Monitoring Service in accordance with its requirements, the scope of such requirements to be reviewed by the Director;

5.2.6 assisting the Central Security Monitoring Service to establish and manage a baseline of network operations and expected data flows for Users and systems, with monthly reporting if requested;

5.2.7 implementing appropriate countermeasures based on threat intelligence disseminated by the Central Security Monitoring Service; and

5.2.8 participating in testing of response and recovery plans coordinated by the Central Security Monitoring Service, in respect of attacks spanning the Wider Information Management System.

6 Information Security Approval Statement

6.1 The Supplier must ensure that its Implementation Plan sets out in sufficient detail how it will ensure compliance with the requirements of this Schedule, including any requirements imposed on Sub-contractors by Annex 2, from the first Operational Services Commencement Date.

6.2 The Supplier may not use the Information Management System to Process Director Data unless and until:

6.2.1 the Supplier has procured the conduct of an IT Health Check of the Supplier System by a CHECK Service Provider or a CREST Service Provider in accordance with Paragraph 9.1; and

6.2.2 the Director has issued the Supplier with an Information Security Approval Statement in accordance with the process set out in this Paragraph 6.

6.3 The Supplier shall document in the Security Management Plan how the Supplier and its Sub-contractors shall comply with the requirements set out in this Schedule and the Agreement in order to ensure the security of the Director Data and the Information Management System.

6.4 The Supplier shall prepare and submit to the Director within twenty (20) Working Days of the date of this Agreement, the Security Management Plan, which comprises:

6.4.1 an Information Security Assurance Assessment;

6.4.2 the Required Changes Register;

6.4.3 the Personal Data Processing Statement;

6.4.4 the diagram documenting the Core Information Management System, the Wider Information Management System and the boundary between them created under Paragraph 4.2; and

6.4.5 the Security Incident Management Process.

6.5 The Director shall review the Supplier's proposed Security Management Plan as soon as possible and, in any event within twenty (20) Working Days of receipt and shall either issue the Supplier with:

6.5.1 an Information Security Approval Statement, which shall confirm that the Supplier may use the Information Management System to Process Director Data; or

6.5.2 a rejection notice, which shall set out the Director's reasons for rejecting the Security Management Plan.

6.6 If the Director rejects the Supplier's proposed Security Management Plan, the Supplier shall take the Director's reasons into account in the preparation of a revised Security Management Plan, which the Supplier shall submit to the Director for review within ten (10) Working Days or such other timescale as agreed with the Director.

6.7 The Director may require, and the Supplier shall provide the Director and its authorised representatives with:

6.7.1 access to the Supplier Personnel;

6.7.2 access to the Core Information Management System to audit the Supplier and its Sub-contractors' compliance with this Agreement; and

6.7.3 such other information and/or documentation that the Director or its authorised representatives may reasonably require,

to assist the Director to establish whether the arrangements which the Supplier and its Sub-contractors have implemented in order to ensure the security of the Director Data and the Information Management System are consistent with the representations in the Security Management Plan. The Supplier shall provide the access required by the Director in accordance with this Paragraph within ten (10) Working Days of receipt of such request, except in the case of a Breach of Security in which

case the Supplier shall provide the Director with the access that it requires within twenty-four (24) hours of receipt of such request.

7 Compliance Reviews

7.1 The Supplier shall regularly review and update the Security Management Plan, and provide such to the Director, at least once each year and as required by this Paragraph. Notwithstanding this general obligation, on a quarterly basis the Supplier shall also review the Customer protection measures in place in accordance with latest sector threats and market research, making proposals to the Director for improvements where appropriate to ensure continued security implementation in line with industry best practice. Where the Director agrees such improvement, the Security Management Plan shall be updated and re-issued.

7.2 The Supplier shall notify the Director within two (2) Working Days after becoming aware of:

7.2.1 a significant change to the components or architecture of the Information Management System;

7.2.2 a new risk to the components or architecture of the Information Management System;

7.2.3 a vulnerability to the components or architecture of the Service which is classified 'Low', 'Medium', 'High' or 'Critical' in accordance with the classification methodology set out in Paragraph 9.3 of Annex 1 to this Schedule;

7.2.4 a change in the threat profile;

7.2.5 a significant change to any risk component;

7.2.6 a significant change in the quantity of Personal Data held within the Service;

7.2.7 a proposal to change any of the Sites from which any part of the Services are provided; and/or

7.2.8 an ISO27001 audit report produced in connection with the Certification Requirements indicates significant concerns.

7.3 Within ten (10) Working Days of notifying the Director in accordance with Paragraph 7.2 or such other timescale as may be agreed with the Director, the Supplier shall make the necessary changes to the Required Changes Register and submit the updated Required Changes Register the Director for review and approval.

7.4 Where the Supplier is required to implement a change, including any change to the Core Information Management System and/or the Security Management Plan in accordance with the Required Changes Register, the Supplier shall effect such change at its own cost and expense.

8 Certification and other Compliance Requirements

8.1 The Supplier shall be certified as compliant with:

8.1.1 ISO/IEC 27001:2013 by a United Kingdom Accreditation Service-approved certification body or is included within the scope of an existing certification of compliance with ISO/IEC 27001:2013; and

8.1.2 Cyber Essentials PLUS,

in all respects applicable to the Services, and shall provide the Director with a copy of each such certificate of compliance before the Supplier shall be permitted to receive, store or Process Director Data.

8.2 The Supplier shall comply with all applicable elements of the NIST Cyber Security Framework. Such compliance shall be subject to annual review by an appointed independent third party, such appointment to be agreed by the Director, to ensure the Supplier's achievement of a minimum of Maturity Level 4 in NIST PRISMA. Any appointment and/or review conducted pursuant to this Paragraph shall be at the Supplier's cost. Unless otherwise expressly agreed in writing by the Director, the Supplier shall also ensure the compliance of all Sub-contractors with the obligation under this Paragraph.

8.3 Unless otherwise expressly agreed in writing by the Director, the Supplier shall ensure that each Sub-contractor is certified as compliant with:

8.3.1 ISO/IEC 27001:2013 by a United Kingdom Accreditation Service-approved certification body or is included within the scope of an existing certification of compliance with ISO/IEC 27001:2013; and

8.3.2 Cyber Essentials PLUS,

in all respects applicable to the Services, and shall provide the Director with a copy of each such certificate of compliance before the Sub-contractor shall be permitted to receive, store or Process Director Data. Notwithstanding this, the Supplier shall ensure that each Sub-contractor is certified compliant with Cyber Essentials at a minimum.

8.4 The Supplier shall ensure that the Supplier and each Sub-contractor who is responsible for the secure destruction of Director Data:

8.4.1 securely destroys Director Data only on Sites which are included within the scope of an existing certification of compliance with ISO/IEC 27001:2013; and

8.4.2 are certified as compliant with the NCSC Assured Service (CAS) Service Requirement Sanitisation Standard or an alternative standard as agreed by the Director,

and evidence of any such destruction shall be provided promptly to the Director on request.

8.5 The Supplier shall provide the Director with evidence of its and its Sub-contractor's compliance with the requirements set out in this Paragraph 8 before the Supplier or the relevant Sub-contractor (as applicable) may carry out the secure destruction of any Director Data.

8.6 The Supplier shall notify the Director as soon as reasonably practicable and, in any event within two (2) Working Days, if the Supplier or any Sub-contractor ceases to be compliant with the Certification Requirements and, on request from the Director, shall or shall procure that the relevant Sub-contractor shall:

8.6.1 immediately cease using the Director Data; and

8.6.2 procure that the relevant Sub-contractor promptly returns, destroys and/or erases the Director Data in accordance with the requirements set out in this Paragraph,

and evidence of any action taken under this Paragraph shall be provided promptly to the Director on request.

8.7 The Director may agree to exempt, in whole or part, the Supplier or any Sub-contractor from the requirements of this Paragraph 8. Any exemption must be in writing to be effective. The Supplier must include the exemption in the Security Management Plan.

9 Security Testing

9.1 The Supplier shall, at its own cost and expense:

9.1.1 procure testing of the Core Information Management System by a CHECK Service Provider or a CREST Service Provider ("**IT Health Check**"):

(a) prior to the first Operational Service Commencement Date and each subsequent Operational Service Commencement Date;

(b) prior to implementation of a significant change;

(c) if directed to do so by the Director; and

(d) once every twelve (12) months during the Term;

9.1.2 conduct vulnerability scanning and assessments of the Core Information Management System monthly;

9.1.3 support testing of the Information Management System end to end solution deployed jointly by the Supplier and other Relevant Third Party Suppliers, on at least an annual basis and otherwise as requested by the Director from time to time;

9.1.4 conduct an assessment as soon as reasonably practicable and in any event within forty-eight (48) hours following publication by a supplier of a vulnerability alert rated 'High' or 'Critical', or within five (5) Working Days following publication by a supplier of a vulnerability alert rated 'Medium' or 'low' affecting any software or other component of the Core Information Management System to determine whether the vulnerability affects the Core Information Management System;

9.1.5 conduct such other tests as are required by:

(a) any Vulnerability Correction Plans;

(b) the ISO27001 certification requirements;

(c) the Security Management Plan; and

(d) the Director following a Breach of Security or a significant change to the components or architecture of the Core Information Management System;

9.1.6 conduct Red Team and Purple Team testing on an annual basis; and

9.1.7 such other security tests, including GBEST testing, as may be required by the Director from time to time,

(each a "**Security Test**").

9.2 The Supplier shall provide the Director and, where requested by the Director or otherwise required pursuant to Paragraph 9.4, the Central Security Monitoring Service, with the results of such Security Tests (in a form approved by the Director in advance) as soon as practicable, and in any case within ten (10) Working Days, after completion of each Security Test.

9.3 In relation to each IT Health Check, the Supplier shall:

9.3.1 agree with the Director the aim and scope of the IT Health Check; and

9.3.2 promptly, and no later than ten (10) Working Days, following the receipt of each IT Health Check report, provide the Director with a copy of the full report, which may be shared with the Central Security Monitoring Service at the Director's discretion.

9.4 In the event that the any of the Security Tests, scanning or assessments (including the IT Health Check report) carried out under Paragraph 9.1 identifies any vulnerabilities or findings (which shall be

categorised in accordance with the CVSS severity levels referred to at Paragraph 9.3 of Annex 1 or, to the extent any such vulnerability or finding does not fit within these categorisations, they shall be categorised at the discretion of the Director), the Supplier shall notify the Director and provide the results, notification of the vulnerabilities or findings to the Central Security Monitoring Service and shall further:

9.4.1 prepare a remedial plan for approval by the Director (each a "**Vulnerability Correction Plan**") which sets out in respect of each vulnerability or finding identified:

(a) how the vulnerability or finding will be remedied or, if the Supplier believes that the risk associated with the vulnerability should be tolerated, document the nature of the vulnerability and the argument for tolerating the risk, to be reviewed and determined in the absolute discretion of the Director;

(b) unless otherwise agreed in writing between the Parties, the date by which the vulnerability or finding will be remedied, which must be:

(i) within five (5) days for those vulnerabilities categorised as “Critical”;

(ii) within fourteen (14) days for those vulnerabilities categorised as “High”; and

(iii) within a timeframe agreed with the Director for those vulnerabilities categorised as “Other”; and

(c) the tests which the Supplier shall perform or procure to be performed (which may, at the discretion of the Director, include a further IT Health Check) to confirm that the vulnerability or finding has been remedied;

9.4.2 comply with the Vulnerability Correction Plan; and

9.4.3 conduct such further tests on the Service as are required by the Vulnerability Correction Plan to confirm that the Vulnerability Correction Plan has been complied with, providing evidence of such compliance promptly on request.

9.5 The Supplier shall ensure that any testing which could adversely affect the Supplier System shall be designed and implemented by the Supplier so as to minimise the impact on the delivery of the Services and the End to End Service and the date, timing, content and conduct of such tests shall be agreed in advance with the Director.

9.6 If any testing conducted by or on behalf of the Supplier identifies a new risk, new threat, vulnerability or exploitation technique that has the potential to affect the security of the Information Management System, the Supplier shall within two (2) Working Days of becoming aware of such risk, threat, vulnerability or exploitation technique provide the Director and the Central Security Monitoring Service with a copy of the test report and:

9.6.1 propose interim mitigation measures to vulnerabilities in the Information Management System known to be exploitable where a security patch is not immediately available; and

9.6.2 where and to the extent applicable, remove or disable any extraneous interfaces, services or capabilities that are not needed for the provision of the Services (in order to reduce the attack surface of the Supplier System) within the timescales set out in the test report or such other timescales as may be agreed with the Director.

9.7 The Supplier shall conduct such further tests of the Supplier System as may be required by the Director from time to time to demonstrate compliance with its obligations set out this Schedule and the Agreement.

9.8 The Supplier shall notify the Director immediately if it fails to, or believes that it will not, mitigate the vulnerability within the timescales set out in Annex 1 to this Schedule 2.4 (*Security Management*).

10 Security Monitoring and Reporting

10.1 Subject always to its overarching obligation to work collaboratively with the Central Security Monitoring Service, the Supplier shall:

10.1.1 monitor the delivery of assurance activities;

10.1.2 maintain and update the Security Management Plan in accordance with Paragraph 7;

10.1.3 agree a document which presents the residual security risks to inform the Director's decision to give approval to the Supplier to Process, store and transit the Director Data;

10.1.4 monitor security risk impacting upon the operation of the Service;

10.1.5 report Breaches of Security in accordance with the approved Security Incident Management Process;

10.1.6 provide to the Director a retrospective monthly report on all incidents, breaches of Security and near misses in respect of the Core Information Management System occurring in that month, to be reviewed by the Director's relevant governance body; and

10.1.7 unless otherwise specified in this Schedule, agree with the Director the frequency and nature of the security reports to be prepared and submitted by the Supplier to the Director within twenty (20) Working Days of the Effective Date.

11 Malicious Software

11.1 The Supplier shall install and maintain an Anti-Malicious Solution or procure that an Anti-Malicious Solution is installed and maintained across the Core Information Management System and ensure that such Anti-Malicious Solution is configured to:

11.1.1 use machine learning/artificial intelligence (AI) to determine if machine behaviour represents a threat;

11.1.2 use a behavioural AI engine to protect against file-less threats;

11.1.3 detect zero-day attacks; and

11.1.4 use cloud-based architecture without need for additional hardware or software.

11.2 If Malicious Software is found, the parties shall cooperate to reduce the effect of the Malicious Software and, particularly if Malicious Software causes loss of operational efficiency or loss or corruption of Director Data, assist each other to mitigate any Losses and to restore the Services to their desired operating efficiency.

11.3 Any cost arising out of the actions of the parties taken in compliance with the provisions of Paragraph 11.2 shall be borne by the parties as follows:

11.3.1 by the Supplier where the Malicious Software originates from the Supplier Software, the Third Party Software supplied by the Supplier or the Director Data (whilst the Director Data was under the control of the Supplier) unless the Supplier can demonstrate that such Malicious Software was present and not quarantined or otherwise identified by the Director when provided to the Supplier; and

11.3.2 by the Director, in any other circumstance.

12 Breach of Security

12.1 The Parties recognise that, notwithstanding the provisions of this Agreement to avoid Breaches of Security, it is likely that Breaches will occur during the Term. The Supplier also recognises that management of Breaches of Security across the Wider Information Management System will be dependent on collaboration with Relevant Third Party Suppliers and the Central Security Monitoring Service, and that time is of the essence in managing Breaches of Security.

12.2 If either Party becomes aware of a Breach of Security or an attempted or suspected Breach of Security, it shall notify the other in accordance with, and to the timescales established in, the Security Incident Management Process set out in the Security Management Plan.

12.3 The Security Incident Management Process set out in the Security Management Plan shall, as a minimum, require:

12.3.1 establishment of an incident response capability, with roles and responsibilities allocated to named and suitably qualified individuals ("**Responders**"), whose details shall be shared with the Director and the Central Security Monitoring Service, and continuity plans ensuring 24/7 resource availability;

12.3.2 production and maintenance of incident response and recovery plans and strategies for all security incidents, including both identified and unidentified incidents, with a priority agreed with the Director based on the risk posted to the security of the Core Information Management System, and ensure that plans and strategies are communicated to Responders and are updated in light of lessons learned from any Breach of Security (such updates to be made as soon as possible and in any event within two (2) weeks of such incident);

12.3.3 the sharing of threat intelligence with the Director, the Central Security Monitoring Service, Relevant Third Party Suppliers and other relevant parties including NSCS; and

12.3.4 configuration of the Supplier's monitoring system to identify any suspected Breach of Security.

12.4 In addition to the requirements in Paragraph 12.3, the Security Incident Management Process shall, as a minimum, require the Supplier to do the following upon it becoming aware of a Breach of Security or attempted Breach of Security:

12.4.1 immediately make available suitably skilled and experienced resource to engage in diagnosis, investigation and response planning, in collaboration with the Director and other parties (including the Central Security Monitoring Service and/or Relevant Third Party Suppliers) as appropriate, even where the attempted or suspected Breach of Security is not believed to have arisen within the Core Information Management System;

12.4.2 immediately communicate the Breach of Security or attempted or suspected Breach of Security to the Director, Central Security Monitoring Service and other parties as directed by the Director, providing such information on the matter as requested by those parties;

12.4.3 identify whether it is a Breach of Security or attempted or suspected Breach of Security, categorise the type of incident against an incident response plan and implement that plan;

12.4.4 immediately take all reasonable steps (which shall include any action or changes reasonably required by the Director or the Central Security Monitoring Service which shall be completed within such timescales as the Director or the Central Security Monitoring Service may reasonably require) necessary to:

(a) minimise the extent of actual or potential harm caused by such Breach of Security;

(b) remedy such Breach of Security to the extent possible and protect the integrity of the Information Management System against any such potential or attempted Breach of Security;

(c) apply a tested mitigation against any such Breach of Security or potential or attempted Breach of Security;

(d) communicate its recovery activities to the Director and the Central Security Monitoring Service and, to the extent required to avoid impact on the Wider Information Management System, to Relevant Third Party Suppliers; and

(e) support any subsequent investigation and preserve evidence as necessary for legal, disciplinary or other reason, including where necessary using forensic analysis techniques; and

12.4.5 as soon as reasonably practicable and, in any event, within ten (10) Working Days following the Breach of Security or attempted Breach of Security, provide to the Director and Central Security Monitoring Service full details of the Breach of Security or attempted Breach of Security, including, where required by the Director or Central Security Monitoring Service, a root cause and impact analysis and/or event data about attempted connections by unauthorised personnel, devices or software, and updating security incident response plans to establish the severity and to prevent a further Breach of Security or attempted Breach of Security in the future exploiting the same root cause failure.

12.5 In the event that any action is taken in response to a Breach of Security or attempted Breach of Security as a result of non-compliance by the Supplier, its Sub-contractors and/or all or any part of the Core Information Management System with this Agreement, then such remedial action shall be completed at no additional cost to the Director.

ANNEX 1: SECURITY REQUIREMENTS

1 Security Classification of Information

1.1 If the provision of the Services requires the Supplier to Process Director Data which is classified as OFFICIAL-SENSITIVE, the Supplier shall implement such additional measures as agreed with the Director from time to time in order to ensure that such information is safeguarded in accordance with the applicable Standards.

2 End User Devices

2.1 The Supplier shall ensure that any Director Data which resides on a mobile, removable or physically uncontrolled device is stored encrypted using a product or system component which has been formally assured through a recognised certification process agreed with the Director except where the Director has given its prior written consent to an alternative arrangement.

2.2 The Supplier shall ensure that any device forming part of the Core Information Management System which is used to Process Director Data meets all of the security requirements set out in the NCSC End User Devices Platform Security Guidance, a copy of which can be found at: https://www.ncsc.gov.uk/collection/end-user-device-security.

3 Networking

3.1 The Supplier shall protect the confidentiality, integrity and availability of Director Data, ensuring it is encrypted in transit and at rest. For the avoidance of doubt, any Director Data which the Supplier causes to be transmitted over any public network (including the Internet, mobile networks or un-protected enterprise network) or to a mobile device shall be encrypted when transmitted.

4 Personnel Security

4.1 All Supplier Personnel shall be subject to a pre-employment check before they may participate in the provision and or management of the Services, and shall be subject to repeat checks periodically according to the Director's policy from time to time. Such pre-employment checks must include all pre-employment checks which are required by the HMG Baseline Personnel Security Standard as in force from time to time including: verification of the individual's identity; verification of the individual's nationality and immigration status; verification of the individual's employment history; and, verification of the individual's criminal record.

4.2 The Director and the Supplier shall review the roles and responsibilities of the Supplier Personnel who will be involved in the management and/or provision of the Services in order to enable the Director to determine which roles require additional vetting and a specific national security vetting clearance (e.g. a Counter Terrorist Check; a Security Check or any equivalent or similar requirement in place from time to time), and shall implement and maintain those checks as notified by the Director. Roles which are likely to require additional vetting and a specific national security vetting clearance include:

4.2.1 system administrators whose role would provide those individuals with privileged access to IT systems which Process Director Data or data which, if it were Director Data, would be classified as OFFICIAL-SENSITIVE;

4.2.2 Supplier Personnel with Enhanced Privileges (root, system administrator, database administrator or equivalent) which enable access to live Bulk Customer Data or copies of the live Bulk Customer Data;

4.2.3 Supplier Personnel working in an information security role or with responsibility for managing information security personnel;

4.2.4 Supplier Personnel working in a financial crime role where those individuals have access to details relating to criminal investigations or with responsibility for managing financial crime personnel; and

4.2.5 Supplier Personnel roles with non-administrative/privileged access to Bulk Customer Data.

4.3 The Supplier shall not permit Supplier Personnel who fail the security checks required by Paragraphs 4.1 and 4.2 to be involved in the management and/or provision of the Services except where the Director has expressly agreed in writing to the involvement of the named individual in the management and/or provision of the Services.

4.4 The Supplier shall ensure that Supplier Personnel are only granted such access to Director Data as is necessary to enable the Supplier Personnel to perform their role and to fulfil their responsibilities.

4.5 The Supplier shall ensure that Supplier Personnel who no longer require access to the Director Data (e.g. they cease to be employed by the Supplier or any of its Sub-contractors), have their rights to access the Director Data revoked within one (1) Working Day.

4.6 The Supplier shall ensure that Supplier Personnel that have access to the Sites, the IT Environment or the Director Data receive regular training on security awareness that reflects the degree of access those individuals have to the Sites, the IT Environment or the Director Data.

4.7 The Supplier shall ensure that the training provided to Supplier Personnel under Paragraph 4.6 includes training on the identification and reporting of fraudulent communications intended to induce individuals to disclose Personal Data or any other information that could be used, including in combination with other Personal Data or information, or with other techniques, to facilitate unauthorised access to the Sites, the IT Environment or the Director Data ("**phishing**").

4.8 The Supplier shall report to the Director following such periodical checks and assurance activities as referred to in Paragraph 4.1, to verify that:

4.8.1 appropriate physical security measures are in place; and

4.8.2 all cyber security staff and privileged Users and Supplier Personnel understand their roles and responsibilities.

5 Identity, Authentication and Access Control

5.1 The Supplier shall be responsible for identity, authentication and access control across the Core Information Management System. This shall include, but not be limited to, ensuring that:

5.1.1 identities and credentials are issued, managed, verified, validated, revoked and audited for Customers, authorised devices, Users and processes;

5.1.2 identities are proofed and bound to credentials and asserted in interactions;

5.1.3 Customers, Users, devices and other assets (including connection of Services to the Integration Platform) are authenticated commensurate with the risk of the transaction in line with the Director's requirements, including implementation of strong multifactor authentication for all Users and Customers and validation of the accuracy of data being inputted by Customers;

5.1.4 Customers can verify that they are interacting with an authorised service representing the Director, and implementing best practice measures to help them to differentiate between authorised communications and fraudulent communications (including, but not limited to, links in SMS messages issued to Customers);

5.1.5 remote access to the Core Information Management System, including remote maintenance, is securely managed using multifactor authentication and performed in a manner that prevents unauthorised access and abuse of administrative access;

5.1.6 maintenance of organisational assets is approved, logged and performed in a manner that prevents unauthorised access and abuse of administrative access;

5.1.7 the Services are delivered from locations which are assessed and approved for compliance to ISO 27001 and HMG standards; and

5.1.8 physical access to assets and the sites from which Services are delivered is managed and protected, and limited to identified, authorised and authenticated personnel.

5.2 The Supplier shall apply the 'principle of least privilege' when allowing persons access to the Supplier System and Sites, using role-based access controls, so that such persons are allowed access only to those parts of the Sites and the Supplier System they require, and the 'principle of separation of duties' to reduce the potential damage from breach of trust by one person. The Supplier shall review and where necessary revoke access permissions where no longer needed, subject to Director approval. The Supplier shall revoke access rights of Users immediately on leaving their role.

5.3 In addition to the obligation under Paragraph 5.2 of this Annex 1, the Supplier shall ensure that Customers' access and ability to carry out activities through the Supplier System and on any Sites (as appropriate) is limited such that they have the ability to act only within their proper entitlement and to ensure appropriate prohibitions and restrictions to prevent activities outside of the boundary of their entitlement.

5.4 The Supplier shall retain records of access to the Sites and to the Supplier System and shall make such record available to the Director on request.

5.5 The Supplier shall:

5.5.1 proactively monitor the internet to identify any fake or scam websites attempting to impersonate the Director and/or associated authorised services, promptly reporting any such identified sites to the Director and to a third party scam website reporting service, ensuring action is taken as necessary to remove any malicious sites;

5.5.2 forward any suspicious email communications received to a third party reporting service, ensuring action is taken as necessary to investigate and remove scam email addresses and websites;

5.5.3 implement measures in line with relevant NCSC guidance to counter use of fake emails purporting to come from within the IT Environment, including use of the latest versions of DMARC, SPF and DKIM;

5.5.4 monitor the physical environment to detect potential instances of unauthorised access or other security events and promptly report any such potential events to the Central Security Monitoring Service; and

5.5.5 monitor Supplier Personnel activity to detect potential instances of unauthorised access or potential or attempted Breaches of Security.

6 Data Destruction or Deletion

6.1 The Supplier shall:

6.1.1 prior to securely sanitising any Director Data or when requested the Supplier shall provide the Director with all Director Data in an agreed open format;

6.1.2 have documented processes to ensure the availability of Director Data in the event of the Supplier ceasing to trade;

6.1.3 securely erase in a manner agreed with the Director any or all Director Data held by the Supplier when requested to do so by the Director;

6.1.4 securely destroy in a manner agreed with the Director all media that has held Director Data at the end of life of that media in accordance with any specific requirements in this Agreement and, in the absence of any such requirements, as agreed by the Director; and

6.1.5 implement processes which address the CPNI and NCSC guidance on secure sanitisation,

and shall promptly provide evidence of compliance with any obligation under this Paragraph 6 as requested by the Director.

7 Audit and Protective Monitoring

7.1 The Supplier shall collect audit records which relate to security events in the Core Information Management System or that would support the analysis of potential and actual compromises. In order to facilitate effective monitoring and forensic readiness such Supplier audit records should (as a minimum) include regular reports and alerts setting out details of access by Users of the Core Information Management System or machine behaviour, to enable the identification of (without limitation) changing access trends, any unusual patterns of usage and/or accounts accessing higher than average amounts of Director Data.

7.2 Notwithstanding the requirement on audit records in Paragraph 7.1 above, the Supplier shall;

7.2.1 within five (5) Working Days of the end of each month during the Term, provide the Director with a written report which details both patched and outstanding vulnerabilities in the Core Information Management System, the elapsed time between the public release date of patches and either time of application or for outstanding vulnerabilities the time of issue of such report and any failure to comply with the timescales set out in Paragraph 9.4 for applying patches to vulnerabilities in the Core Information Management System; and

7.2.2 provide to the Director a monthly report on the presence of all publicly disclosed vulnerabilities, or those notified by the Director, affecting systems directly involved in the delivery of the Services. For vulnerabilities classed as high severity (7 or higher) by the CVSS, the Supplier shall notify the Director within forty-eight (48) hours of disclosure. For medium severity vulnerabilities, the Supplier shall notify the Director within five (5) Working Days of disclosure.

7.3 The Supplier and the Director shall work together to establish any additional audit and monitoring requirements for the Core Information Management System and the Supplier shall continually improve monitoring processes in line with Good Industry Practice and in accordance with any instruction from the Director.

7.4 Retention periods for audit records and event logs must be agreed with the Director and documented in the Security Management Plan.

8 Location of Director Data

8.1 The Supplier shall not and shall procure that none of its Sub-contractors Process Director Data outside the United Kingdom without the prior written consent of the Director, which may be subject to conditions.

9 Threats, Vulnerabilities and Corrective Action

9.1 The Director and the Supplier acknowledge that from time to time vulnerabilities in the Core Information Management System will be discovered which unless mitigated will present an unacceptable risk to the Director.

9.2 The Director and the Supplier also acknowledge the importance of remaining alert to the range of threats posed to the Service by threat actors, and the imperative to understand and counteract these threats as far as practicable.

9.3 The severity of vulnerabilities for COTS Software shall be categorised by the Supplier as 'Critical', 'High', 'Medium' and 'Low' by aligning these categories to the vulnerability scoring using the National Vulnerability Database's 'Vulnerability Severity Ratings' (CVSS v3.0 scores as set out by NIST at http://nvd.nist.gov/cvss.cfm).

9.4 Subject to Paragraph 9.5, the Supplier shall apply, or procure the application of security patches to vulnerabilities in the Core Information Management System within:

9.4.1 five (5) days after the public release of patches for those vulnerabilities categorised as 'Critical';

9.4.2 fourteen (14) days after the public release of patches for those vulnerabilities categorised as 'High'; and

9.4.3 within a timeframe agreed with the Director following the public release of patches for those vulnerabilities categorised as 'Other'.

9.5 The timescales for applying patches to vulnerabilities in the Core Information Management System set out in Paragraph 9.4 shall be extended where:

9.5.1 the Supplier can demonstrate that a vulnerability in the Core Information Management System is not exploitable within the context of the Services (e.g. because it resides in a Software component which is not involved in running in the Services) provided such vulnerabilities shall be remedied by the Supplier within the timescales set out in Paragraph 9.4 if the vulnerability becomes exploitable within the context of the Services;

9.5.2 the application of a 'Critical' or 'High' security patch adversely affects the Supplier's ability to deliver the Services in which case the Supplier shall be granted an extension to such timescales of five (5) days, provided the Supplier had followed and continues to follow the security patch test plan agreed with the Director; or

9.5.3 the Director agrees a different maximum period after a case-by-case consultation with the Supplier under the processes defined in the Security Management Plan.

The Security Management Plan shall include provisions for major version upgrades of all COTS Software to be kept up to date such that all COTS Software are always in mainstream support throughout the Term unless otherwise agreed by the Director in writing. All components used to deliver the Services, including hardware and COTS Software, should be maintained at mainstream supported levels.

9.6 The Supplier shall provide a means for Users and Customers alike to report security vulnerabilities or issues, using such feedback to inform future development of Services.

10 Secure Architecture

10.1 The Supplier shall ensure that all Services are designed, developed and deployed:

10.1.1 to be 'Secure by Default' in line with NCSC guidance;

10.1.2 in accordance with the NIST Secure Software Development Framework (SSDF);

10.1.3 where Customer-facing:

(a) application development, in compliance with the OWASP Application Security Verification Standard;

(b) mobile application development, in compliance with the OWASP Mobile Application Security Verification Standard,

and in each case validated through the software development and deployment systems and evidenced to the Director through the security reporting process.

10.2 The Supplier shall design the Core Information Management System in accordance with:

10.2.1 the NCSC "Security Design Principles for Digital Services", a copy of which can be found at: https://www.ncsc.gov.uk/guidance/security-design-principles-digital-services-main;

10.2.2 the NCSC "Bulk Data Principles", a copy of which can be found at https://www.ncsc.gov.uk/guidance/protecting-bulk-personal-data-main; and

10.2.3 the NSCS "Cloud Security Principles", a copy of which can be found at: https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles and which are summarised below:

(a) "Cloud Security Principle 1: data in transit protection" which, amongst other matters, requires that user data transiting networks should be adequately protected against tampering and eavesdropping;

(b) "Cloud Security Principle 2: asset protection and resilience" which, amongst other matters, requires that user data, and the assets storing or processing it, should be protected against physical tampering, loss, damage or seizure;

(c) "Cloud Security Principle 3: separation between users" which, amongst other matters, requires that a malicious or compromised user of the service should not be able to affect the service or data of another;

(d) "Cloud Security Principle 4: governance framework" which, amongst other matters, requires that the Supplier should have a security governance framework which coordinates and directs its management of the Services and information within it;

(e) "Cloud Security Principle 5: operational security" which, amongst other matters, requires that the Services need to be operated and managed securely in order to impede, detect or prevent a Breach of Security;

(f) "Cloud Security Principle 6: personnel security" which, amongst other matters, requires that where Supplier Personnel have access to Director Data and/or the Director System that those personnel be subject to appropriate security screening and regular security training;

(g) "Cloud Security Principle 7: secure development" which, amongst other matters, requires that the Services be designed and developed to identify and mitigate threats to their security;

(h) "Cloud Security Principle 8: supply chain security" which, amongst other matters, requires the Supplier to ensure that appropriate security controls are in place with its Sub-contractors and other suppliers;

(i) "Cloud Security Principle 9: secure user management" which, amongst other matters, requires the Supplier to make the tools available for the Director to securely manage the Director's use of the Service;

(j) "Cloud Security Principle 10: identity and authentication" which, amongst other matters, requires the Supplier to implement appropriate controls in order to ensure that access to Service interfaces is constrained to authenticated and authorised individuals;

(k) "Cloud Security Principle 11: external interface protection" which, amongst other matters, requires that all external or less trusted interfaces with the Services should be identified and appropriately defended;

(l) "Cloud Security Principle 12: secure service administration" which, amongst other matters, requires that any ICT system which is used for administration of a cloud service will have highly privileged access to that service;

(m) "Cloud Security Principle 13: audit information for users" which, amongst other matters, requires the Supplier to be able to provide the Director with the audit records it needs to monitor access to the Service and the Director Data held by the Supplier and/or its Sub-contractors; and

(n) "Cloud Security Principle 14: secure use of the service" which, amongst other matters, requires the Supplier to educate Supplier Personnel on the safe and secure use of the Information Management System.

10.3 The Supplier shall ensure digital design and development activities are undertaken securely so that deployments or any significant changes are done securely and do not pose a security threat to the Director's wider ecosystem.

ANNEX 2: SECURITY REQUIREMENTS FOR SUB-CONTRACTORS

1 Application of Annex

1.1 This Annex applies to all Sub-contractors that Process Director Data.

1.2 The Supplier must:

1.2.1 ensure that those Sub-contractors comply with the provisions of this Annex;

1.2.2 keep sufficient records to demonstrate that compliance to the Director; and

1.2.3 ensure that its Implementation Plan includes Deliverable Items, Milestones and Milestone Dates that relate to the design, implementation and management of any systems used by Sub-contractors to Process Director Data.

2 Designing and managing secure solutions

2.1 The Sub-contractor shall implement their solution(s) to mitigate the security risks in accordance with the NCSC's Cyber Security Design Principles https://www.ncsc.gov.uk/collection/cyber-security-design-principles.

2.2 The Sub-contractor must assess their systems against the NCSC Cloud Security Principles: https://www.ncsc.gov.uk/collection/cloud-security?curPage=/collection/cloud-security/implementing-the-cloud-security-principles at their own cost and expense to demonstrate that the people, process, technical and physical controls have been delivered in an effective way. The Sub-contractor must document that assessment and make that documentation available to the Director on the Director's request.

3 Data Processing, Storage, Management and Destruction

3.1 The Sub-contractor must not Process any Director Data outside the United Kingdom. The Director may permit the Sub-contractor to Process Director Data outside the United Kingdom and may impose conditions on that permission, with which the Sub-contractor must comply. Any permission must be in writing to be effective.

3.2 The Sub-contractor must securely erase any or all Director Data held by the Sub-contractor when requested to do so by the Director; and, securely destroy all media that has held Director Data at the end of life of that media in accordance with the NCSC Assured Service (CAS) Service Requirement Sanitisation Standard, or an alternative agreed in writing by the Director.

4 Personnel Security

4.1 The Sub-contractor must perform appropriate checks on their staff before they may participate in the provision and or management of the Services, and shall be subject to repeat checks periodically according to the Director's policy from time to time. Those checks must include all pre-employment checks required by the HMG Baseline Personnel Security Standard including: verification of the individual's identity; verification of the individual's nationality and immigration status; verification of the individual's employment history; and verification of the individual's criminal record. The HMG Baseline Personnel Security Standard is at https://www.gov.uk/government/publications/government-baseline-personnel-security-standard.

4.2 The Sub-contractor must, if the Director requires, at any time, ensure that one or more of the Sub-contractor's staff obtains Security Check clearance in order to Process Director Data containing Personal Data above certain volumes specified by the Director, or containing Special Category Personal Data.

4.3 Any Sub-contractor staff who will, when performing the Services, have access to a person under the age of eighteen (18) years must undergo Disclosure and Barring Service checks.

4.4 The Supplier and the Sub-contractor shall review the roles and responsibilities of the Sub-contractor staff who will be involved in the management and/or provision of the Services in order to determine which roles require additional vetting and a specific national security vetting clearance (e.g. a Counter Terrorist Check; a Security Check or any equivalent or similar requirement in place from time to time), and shall implement and maintain those checks. Roles which are likely to require additional vetting and a specific national security vetting clearance include:

4.4.1 System administrators whose role would provide those individuals with privileged access to IT systems which Process Director Data or data which, if it were Director Data, would be classified as OFFICIAL-SENSITIVE;

4.4.2 Sub-contractor staff with Enhanced Privileges (root, system administrator, database administrator or equivalent) which enable access to live Bulk Customer Data or copies of the live Bulk Customer Data;

4.4.3 Sub-contractor staff working in an information security role or with responsibility for managing information security personnel;

4.4.4 Sub-contractor staff working in a financial crime role where those individuals have access to details relating to criminal investigations or with responsibility for managing financial crime personnel; and

4.4.5 Sub-contractor staff roles with non-administrative/privileged access to Bulk Customer Data where:

(a) access is to full copies of live Bulk Customer Data that allows individuals to be identified;

(b) access is not being controlled by the application to single records only; and

(c) no audit trail of access to information records is created.

4.5 The Sub-contractor shall not permit Sub-contractor staff who fail the security checks required by this Paragraph 4 to be involved in the management and/or provision of the Services except where the Director has expressly agreed in writing to the involvement of the named individual in the management and/or provision of the Services.

4.6 The Sub-contractor shall ensure that Sub-contractor staff are only granted such access to Director Data as is necessary to enable the Sub-contractor staff to perform their role and to fulfil their responsibilities.

4.7 The Sub-contractor shall ensure that Sub-contractor staff who no longer require access to the Director Data (e.g. they cease to be employed by the Sub-contractor), have their rights to access the Director Data revoked within one (1) Working Day.

4.8 The Sub-contractor shall ensure that Sub-contractor staff that have access to the Sites, the IT Environment or the Director Data receive regular training on security awareness that reflects the degree of access those individuals have to the Sites, the IT Environment or the Director Data.

4.9 The Sub-contractor shall ensure that the training provided to Sub-contractor staff under Paragraph 4.8 includes training on the identification and reporting of fraudulent communications intended to induce individuals to disclose Personal Data or any other information that could be used, including in combination with other Personal Data or information, or with other techniques, to facilitate unauthorised access to the Sites, the IT Environment or the Director Data ("**phishing**").

5 End User Devices

5.1 The Sub-contractor shall ensure that any Director Data stored (for any period of time) on a mobile, removable or physically uncontrolled device is encrypted. The Sub-contractor must follow the Information Commissioner's Office guidance on implementing encryption, which can be found at

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/encryption/.

5.2 The Sub-contractor shall ensure that any device used to Process Director Data meets all the security requirements set out in the NCSC End User Devices Platform Security Guidance, which can be found at: https://www.ncsc.gov.uk/guidance/end-user-device-security.

6 Networking

6.1 The Sub-contractor shall ensure that any Director Data which it causes to be transmitted over any public network (including the Internet, mobile networks or un-protected enterprise network) or to a mobile device shall be encrypted when transmitted.

7 Patching and Vulnerability Scanning

7.1 The Sub-contractor must proactively monitor supplier vulnerability websites and ensure all necessary patches and upgrades are applied to maintain security, integrity and availability in accordance with the NCSC Cloud Security Principles.

8 Third Party Sub-contractors

8.1 The Sub-contractor must not transmit or disseminate the Director Data to any other person unless specifically authorised by the Director. Such authorisation must be in writing to be effective and may be subject to conditions.

8.2 The Sub-contractor must not, when performing any part of the Services, use any software to Process the Director Data where the licence terms of that software purport to grant the licensor rights to Process the Director Data greater than those rights strictly necessary for the use of the software.

ANNEX 3: SECURITY MANAGEMENT PLAN TEMPLATE

Security Management Plan Template (Assurance)

[Project/Service and Supplier Name]

1 Executive Summary

<This section should contain a brief summary of the business context of the system, any key IA controls, the assurance work done, any off-shoring considerations and any significant residual risks that need acceptance.>

2 System Description

2.1 Background

<A short description of the project/product/system. Describe its purpose, functionality, aim and scope.>

2.2 Organisational Ownership/Structure

<Who owns the system and operates the system and the organisational governance structure. This should include how any ongoing security management is integrated into the project governance e.g. how a Security Working Group reports to the project board.>

2.3 Information assets and flows

<The information assets processed by the system which should include a simple high level diagram on one page. Include a list of the type and volumes of data that will be processed, managed and stored within the supplier system. If personal data, please include the fields used such as name, address, department DOB, NI number etc.>

2.4 System Architecture

<A description of the physical system architecture, to include the system management. A diagram will be needed here.>

2.5 Users

<A brief description of the system Users, to include HMG Users as well as any service provider Users and system managers. If relevant, security clearance level requirements should be included.>

2.6 Locations

<Where the data assets are stored and managed from. If any locations hold independent security certifications (e.g. ISO27001:2013) these should be noted. Any off-shoring considerations should be detailed.>

2.7 Test and Development Systems

<Include information about any test and development systems, their locations and whether they contain live system data.>

2.8 Roles and Responsibilities

<A brief description of the lead security roles such as that of the SIRO, IA O, Security manager, Accreditor.>

3 Risk Assessment

3.1 Assurance Scope

<This section describes the scope of the Assurance for the system. The scope of the assurance assessment should be clearly indicated, with components of the architecture upon which reliance is placed but assurance will not be done clearly shown e.g. a cloud hosting service. A logical diagram should be used along with a brief description of the components.>

3.2 Risk appetite

<A risk appetite should be agreed with the SIRO/SRO and included here.>

3.3 Business impact assessment

<A description of the information assets and the impact of their loss or corruption (e.g. large amounts of Official Sensitive personal data the loss of which would be severely damaging to individuals, embarrassing to HMG, and make HMG liable to ICO investigations) in business terms should be included. This section should cover the impact on loss of confidentiality, integrity and availability of the assets. The format of this assessment may be dependent on the risk assessment method chosen.>

3.4 Risk assessment

<The content of this section will depend on the risk assessment methodology chosen, but should contain the output of the formal information risk assessment in a prioritised list using business language. Experts on the system and business process should have been involved in the risk assessment to ensure the formal risk methodology used has not missed out any risks. The example table below should be used as the format to identify the risks and document the controls used to mitigate those risks.>

Risk ID	Inherent risk	Inherent risk level	Vulnerability	Controls	Residual risk level
R1	Internet attackers could hack the system.	Medium	The service systems are exposed to the internet via the web portal.	C1: Internet-facing firewalls C2: Internet-facing IP whitelist C3: System hardening C4: Protective monitoring C5: Application access control C16: Anti-virus for incoming files C54: Files deleted when processed C59: Removal of departmental identifier	Very low

Risk ID	Inherent risk	Inherent risk level	Vulnerability	Controls	Residual risk level
R2	Remote attackers could intercept or disrupt information crossing the internet.	Medium	File sharing with organisations across the internet.	C9: TLS communications C10: PGP file-sharing	Very low
R3	Internal Users could maliciously or accidentally alter bank details.	Medium-High	Customers' bank details can be altered as part of the normal business function.	C12. System administrators hold SC clearance C13. All changes to Customer information are logged and audited C14. Letters are automatically sent to Customers' home addresses when bank details are altered C15. Staff awareness training	Low

3.5 Controls

<The controls listed above to mitigate the risks identified should be detailed. There should be a description of each control, further information and configuration details where relevant, and an assessment of the implementation status of, and assurance in, the control. A sample layout is included below.>

ID	Control title	Control description	Further information and assurance status
C1	Internet-facing firewalls	Internet-facing firewalls are in place between the internet and the system, which restrict access from the internet to the required ports only.	Assured via ITHC firewall rule check
C2	Internet-facing IP whitelist	An IP whitelist is in place for all access from the internet.	Assured via ITHC
C15	Staff awareness training	All staff must undertake annual security awareness training and this process is audited and monitored by line managers.	Assured as part of ISO27001 certification

3.6 Residual risks and actions

<A summary of the residual risks which are likely to be above the risk appetite stated after all controls have been applied and verified should be listed with actions and timescales included.>

4 In-service controls

<This section should describe the controls relating to the information lifecycle, including development, testing, in-service, termination and on-going risk management and accreditation assurance. Details of any formal assurance requirements specified in the contract such as security CHECK testing or maintained ISO27001 certification should be included. This section should include at least:

4.1 information risk management and timescales and triggers for a review;

4.2 contractual patching requirements and timescales for the different priorities of patch;

4.3 protective monitoring arrangements to include how anomalous behaviour is identified and acted upon as well as how logging and auditing of user activity is done;

4.4 configuration and change management;

4.5 incident management;

4.6 vulnerability management;

4.7 user access management; and

4.8 data sanitisation and disposal.>

5 Security Operating Procedures (SyOPs)

<If needed any SyOps requirements should be included and referenced here.>

6 Major Hardware and Software and end of support dates

<This should be a table which lists the end of support dates for hardware and software products and components. An example table is shown below.>

Name	Version	End of mainstream Support/Extended Support	Notes/RAG Status
Server Host	HP XXXX	Feb 2020/ March 2022	

7 Security Incident Management Process

<The Suppliers' process, as agreed with the Director/Customer, should be included here. It must as a minimum include the protocol for how and when incidents will be reported to the Director/Customer and the process that will be undertaken to mitigate the incidents and investigate the root cause.>

8 Security Requirements for User Organisations

<Any security requirements for connecting organisations or departments should be included or referenced here.>

9 Required Changes Register

<The table below shows the headings for the Required Changes Register which should be maintained and used to update the contents of this document at least annually.>

Ref	Section	Change	Agreed With	Date agreed	Documentation update	Status
1	6.4	A new Third Party supplier XXXX will be performing the print capability.	Director name	11/11/2018	Jul-2019	Open

10 Personal Data Processing Statement

<This should include: (i) the types of Personal Data which the Supplier and/or its Sub-contractors are Processing on behalf of the Director; (ii) the categories of Data Subjects whose Personal Data the Supplier and/or its Sub-contractors are Processing on behalf of the Director; the nature and purpose of such Processing; (iii) the locations at which the Supplier and/or its Sub-contractors Process Director Data; and, (iv) the Protective Measures that the Supplier and, where applicable, its Sub-contractors have implemented to protect the Director Data against a Security Breach including a Personal Data Breach.>

11 Annex A. ISO27001 and/or Cyber Essential Plus certificates

<Any certifications relied upon should have their certificates included.>

12 Annex B. Cloud Security Principles assessment

<A spreadsheet may be attached.>

13 Annex C. Protecting Bulk Data assessment if required by the Director/Customer

<A spreadsheet may be attached.>

14 Annex E. Latest ITHC report and Vulnerability Correction Plan

SCHEDULE 2.5 - INSURANCE REQUIREMENTS

1 OBLIGATION TO MAINTAIN INSURANCES

1.1 Without prejudice to its obligations to the Director under this Agreement, including its indemnity and liability obligations, the Supplier shall for the periods specified in this Schedule take out and maintain, or procure the taking out and maintenance of the insurances as set out in Annex 1 and any other insurances as may be required by applicable Law (together the "**Insurances**"). The Supplier shall ensure that each of the Insurances is effective no later than the date on which the relevant risk commences.

1.2 The Insurances shall be maintained in accordance with Good Industry Practice and (so far as is reasonably practicable) on terms no less favourable than those generally available to a prudent contractor in respect of risks insured in the international insurance market from time to time.

1.3 The Insurances shall be taken out and maintained with insurers who are:

1.3.1 of good financial standing;

1.3.2 appropriately regulated;

1.3.3 regulated by the applicable regulatory body and is in good standing with that regulator; and

1.3.4 except in the case of any Insurances provided by an Affiliate of the Supplier, of good repute in the international insurance market.

1.4 The Supplier shall ensure that the public and products liability policy shall contain an indemnity to principals clause under which the Director shall be indemnified in respect of claims made against the Director in respect of death or bodily injury or third party property damage arising out of or in connection with the Agreement and for which the Supplier is legally liable.

2 GENERAL OBLIGATIONS

2.1 Without limiting the other provisions of this Agreement, the Supplier shall:

2.1.1 take or procure the taking of all reasonable risk management and risk control measures in relation to the Services as it would be reasonable to expect of a prudent contractor acting in accordance with Good Industry Practice, including the investigation and reports of relevant claims to insurers;

2.1.2 promptly notify the insurers in writing of any relevant material fact under any Insurances of which the Supplier is or becomes aware;

2.1.3 hold all policies in respect of the Insurances and cause any insurance broker effecting the Insurances to hold any insurance slips and other evidence of placing cover representing any of the Insurances to which it is a party; and

2.1.4 promptly notify the Director and in any event within ten (10) Working Days after it makes any insurance claim in excess of £500,000 against any of the policies below.

3 FAILURE TO INSURE

3.1 The Supplier shall not take any action or fail to take any action or (insofar as is reasonably within its power) permit anything to occur in relation to it which would entitle any insurer to refuse to pay any claim under any of the Insurances.

3.2 Where the Supplier has failed to purchase any of the Insurances or maintain any of the Insurances in full force and effect, the Director may elect (but shall not be obliged) following written notice to the Supplier to purchase the relevant Insurances, and the Director shall be entitled to recover the

reasonable premium and other reasonable costs incurred in connection therewith as a debt due from the Supplier.

4 EVIDENCE OF INSURANCES

4.1 The Supplier shall upon the Effective Date and within fifteen (15) Working Days after the renewal or replacement of each of the Insurances, provide evidence, in a form satisfactory to the Director, that the Insurances are in force and effect and meet in full the requirements of this Schedule. Receipt of such evidence by the Director shall not in itself constitute acceptance by the Director or relieve the Supplier of any of its liabilities and obligations under this Agreement.

5 CANCELLATION

5.1 Subject to Paragraph 5.2, the Supplier shall notify the Director in writing at least five (5) Working Days prior to the cancellation, suspension, termination or non-renewal of any of the Insurances.

5.2 Without prejudice to the Supplier's obligations under Paragraph 4, Paragraph 5.1 shall not apply where the termination of any Insurances occurs purely as a result of a change of insurer in respect of any of the Insurances required to be taken out and maintained in accordance with this Schedule.

6 INSURANCE CLAIMS, PREMIUMS AND DEDUCTIBLES

6.1 The Supplier shall promptly notify to insurers any matter arising from, or in relation to, the Services and/or this Agreement for which it may be entitled to claim under any of the Insurances. In the event that the Director receives a claim relating to or arising out of the Services and/or this Agreement, the Supplier shall co-operate with the Director and assist it in dealing with such claims at its own expense including without limitation providing information and documentation in a timely manner.

6.2 The Supplier shall maintain a register of all claims under the Insurances in connection with this Agreement and shall allow the Director to review such register at any time.

6.3 Where any Insurance requires payment of a premium, the Supplier shall be liable for and shall promptly pay such premium.

6.4 Where any Insurance is subject to an excess or deductible below which the indemnity from insurers is excluded, the Supplier shall be liable for such excess or deductible. The Supplier shall not be entitled to recover from the Director any sum paid by way of excess or deductible under the Insurances whether under the terms of this Agreement or otherwise.

ANNEX 1: REQUIRED INSURANCES

Part 1: INSURANCE CLAIM NOTIFICATION

Except where the Director is the claimant party, the Supplier shall give the Director notice within ten (10) Working Days after any insurance claim in excess of £100,000, relating to or arising out of the provision of the Services or this Agreement, on Technology Professional Indemnity or Cyber Liability Insurance or which, but for the application of the applicable policy excess, would be made on such Insurances and (if required by the Director) full details of the incident giving rise to the claim.

Part 2: TECHNOLOGY PROFESSIONAL INDEMNITY AND CYBER LIABILITY INSURANCE

1 Insured

1.1 The Supplier.

2 Interest

2.1 To indemnify the Insured in respect of:

2.1.1 **Professional Liability** – all sums which the Insured shall become legally liable to pay, including damages and claimant's costs and expenses (including regulatory fines or penalties, data subject breach claims, claimant's costs and expenses), in respect of an actual or suspected defect or deficiency in service or failure to perform in accordance with the terms of this Agreement, including any civil liability, any data protection, security losses and breaches happening during the period of insurance (as specified in Paragraph 5); and

2.1.2 **Cyber** – all sums which the Insured shall become legally liable to pay including, but not limited to damages, claimant's costs and expenses, costs to mitigate or remediate the impact of an attack or data breach or costs incurred in relation to breach of this Agreement in respect of cyber-attacks and breaches of cyber security happening during the period of insurance (as specified in Paragraph 5),

arising out of or in connection with the provision of the Services and in connection with this Agreement.

3 Limit of indemnity

3.1 In respect of Professional Liability, not less than £70 million per event and in the aggregate per annum.

3.2 In respect of Cyber, not less than £50 million per event and in the aggregate per annum.

4 Territorial limit

In respect of Cyber, the territory covered will be worldwide. In respect of Professional Indemnity, the territory covered will be the United Kingdom.

5 Period of insurance

5.1 From the date of this Agreement for the Term and renewable on an annual basis unless agreed otherwise by the Director in writing.

6 Cover features and extensions

6.1 Indemnity to principals clause under which the Director shall be indemnified in respect of claims made against the Director in respect of Cyber Liability insurance arising out of or in connection with the Agreement and for which the Supplier is legally liable.

7 Maximum deductible threshold

Not to exceed [redacted] for each and every Cyber Liability insurance claim.

Part 3: OTHER REQUIRED INSURANCES

Class	Minimum Sum Insured
Third Party Public and Products Liability Insurance	£10 million (per event) / £10 million (aggregate)
Employers' Liability Insurance	£10 million (per event)
Property Damage Insurance	£50 million

SCHEDULE 3 - DIRECTOR RESPONSIBILITIES

1 INTRODUCTION

1.1 The responsibilities of the Director set out in this Schedule shall constitute the Director Responsibilities under this Agreement. Any obligations of the Director in Schedule 2.1 (*Services Description*) and Schedule 4.1 (*Supplier Solution*) shall not be Director Responsibilities and the Director shall have no obligation to perform any such obligations unless they are specifically stated to be "Director Responsibilities" and cross-referenced in the table in Paragraph 3.

1.2 The responsibilities specified within this Schedule shall be provided to the Supplier free of charge, unless otherwise agreed between the Parties.

2 GENERAL OBLIGATIONS

2.1 The Director shall:

2.1.1 perform those obligations of the Director which are set out in the Clauses of this Agreement and the Paragraphs of the Schedules (except Schedule 2.1 (*Services Description*) and Schedule 4.1 (*Supplier Solution*));

2.1.2 use its reasonable endeavours to provide the Supplier with access to appropriate members of the Director's staff, as such access is reasonably requested by the Supplier in order for the Supplier to discharge its obligations throughout the Term and the Termination Assistance Period;

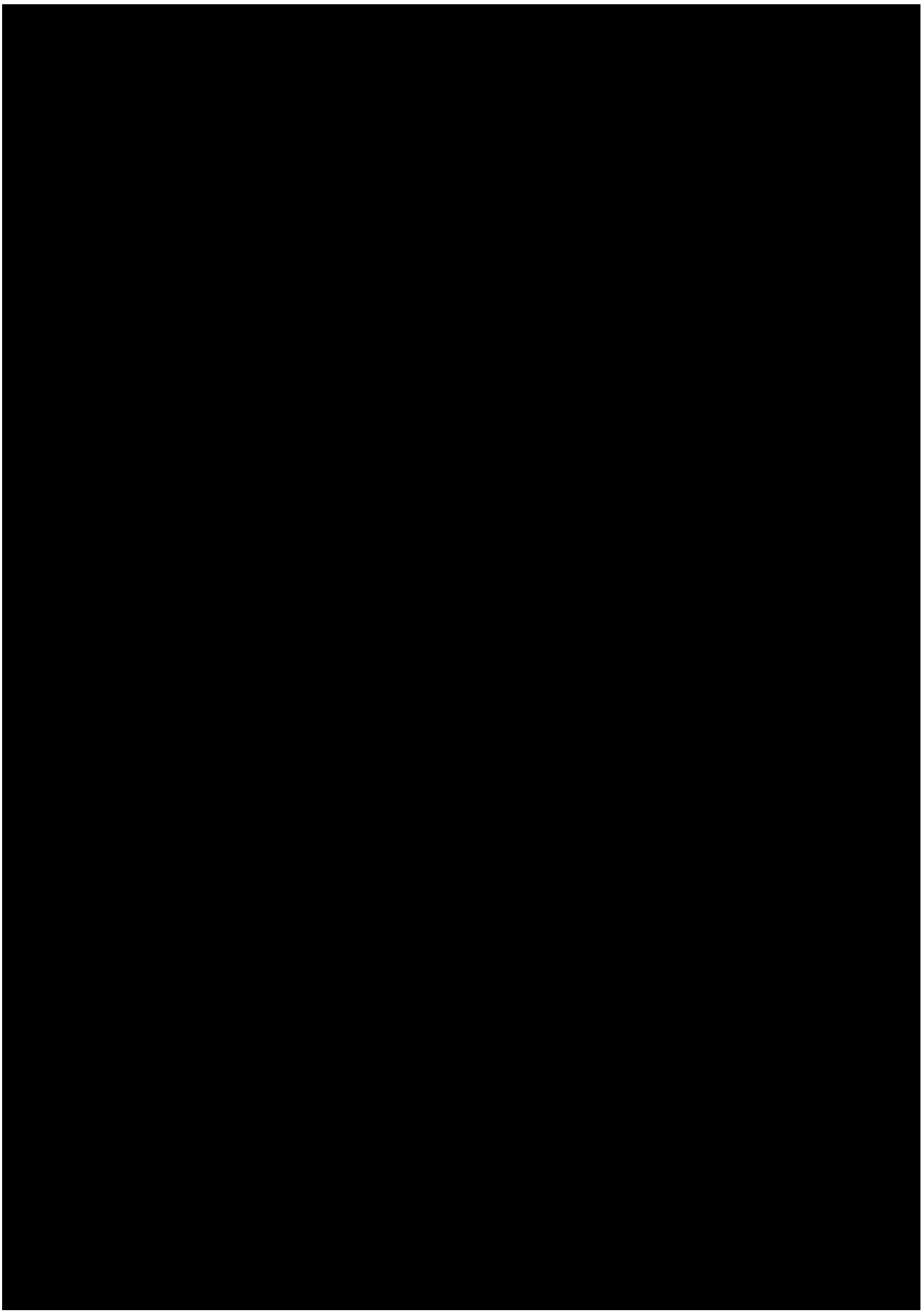
2.1.3 provide sufficient and suitably qualified staff to fulfil the Director's roles and duties under this Agreement as defined in the Implementation Plan;

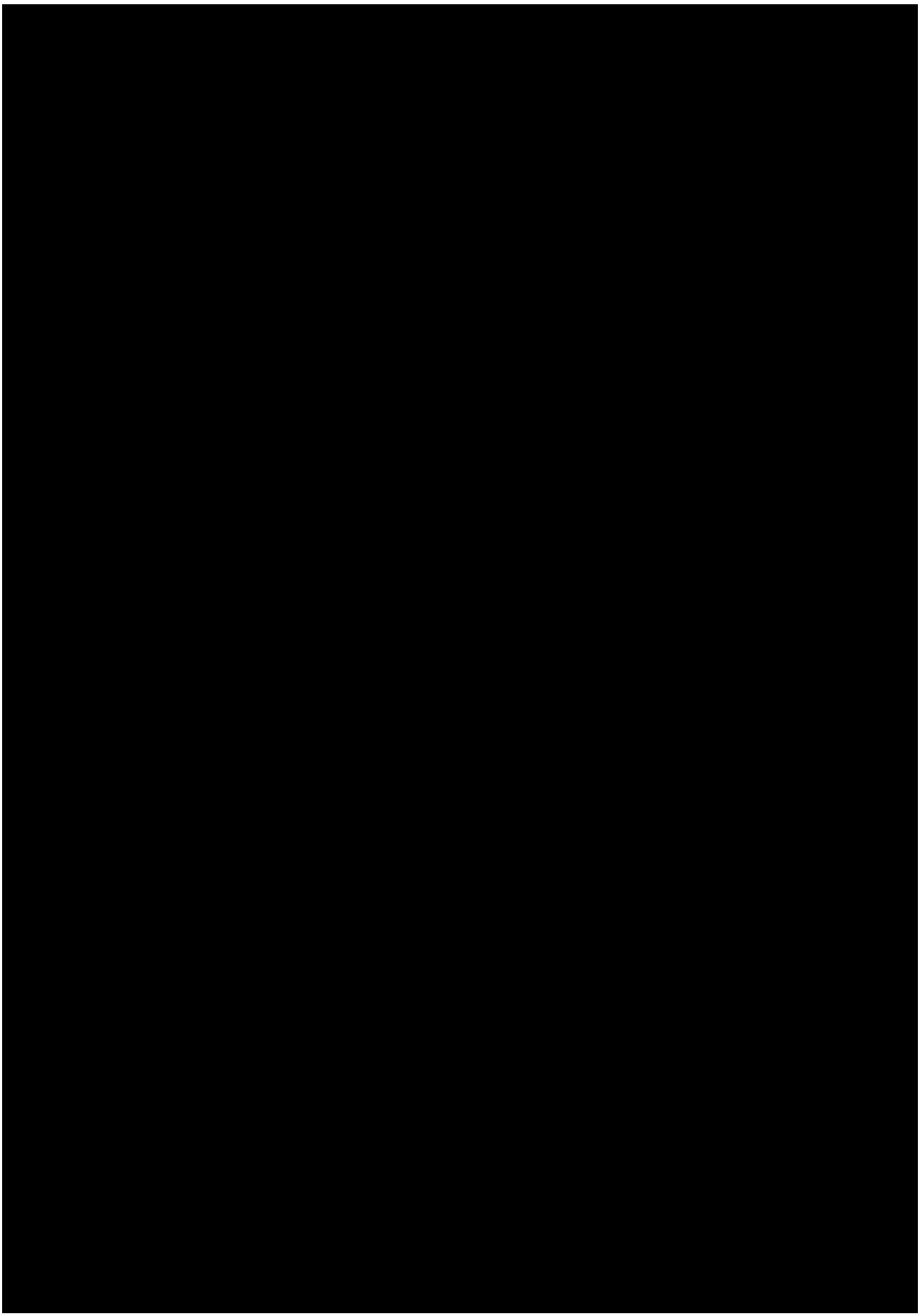
2.1.4 use its reasonable endeavours to provide such documentation, data and/or other information that the Supplier reasonably requests that is necessary to perform its obligations under the terms of this Agreement provided that such documentation, data and/or information is available to the Director and is authorised for release by the Director; and

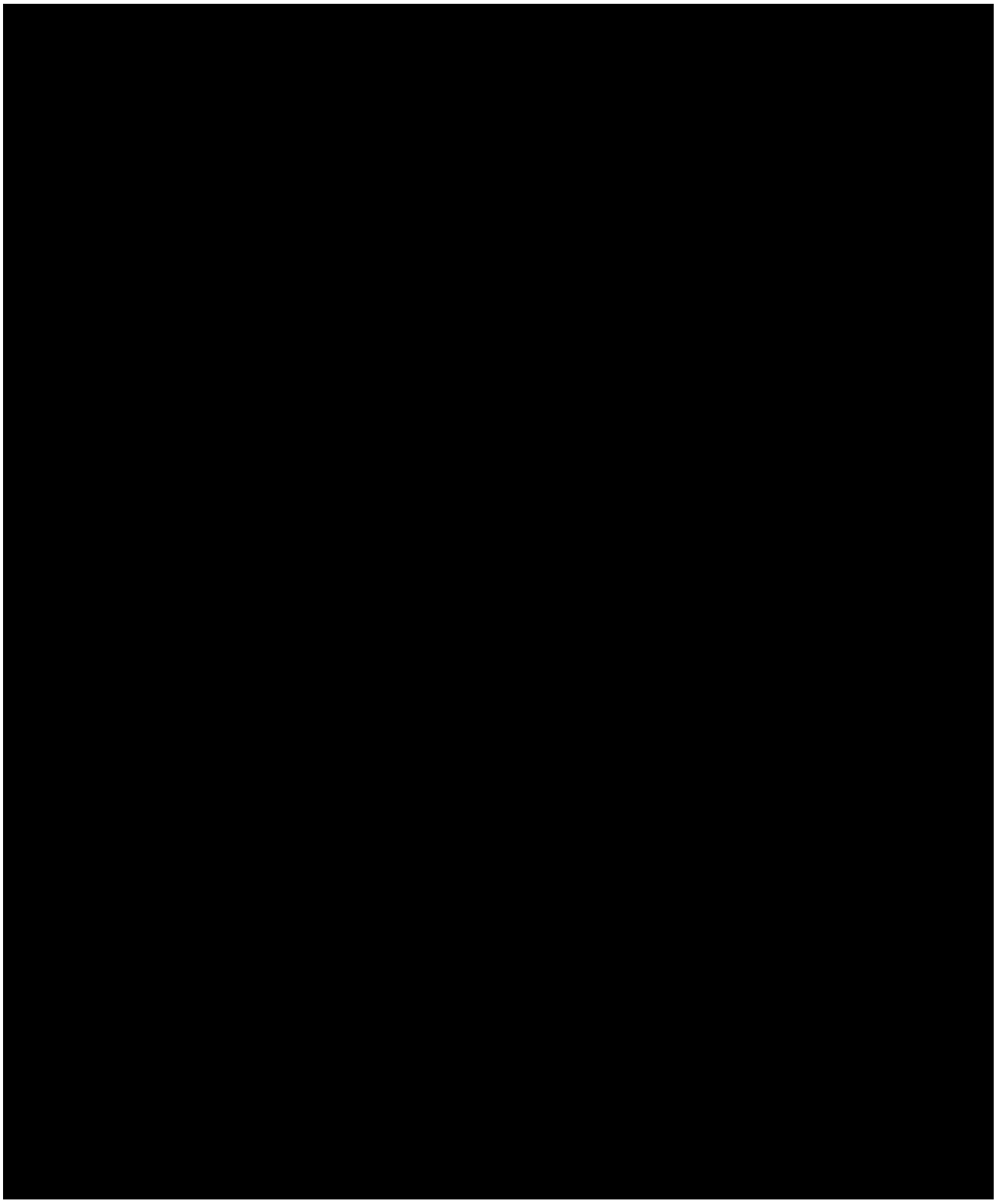
2.1.5 procure for the Supplier such agreed access and use of the Director Premises (as a licensee only) and facilities (including relevant IT systems) as is reasonably required for the Supplier to comply with its obligations under this Agreement, such access to be provided during the Director's normal working hours on each Working Day or as otherwise agreed by the Director (such agreement not to be unreasonably withheld or delayed).

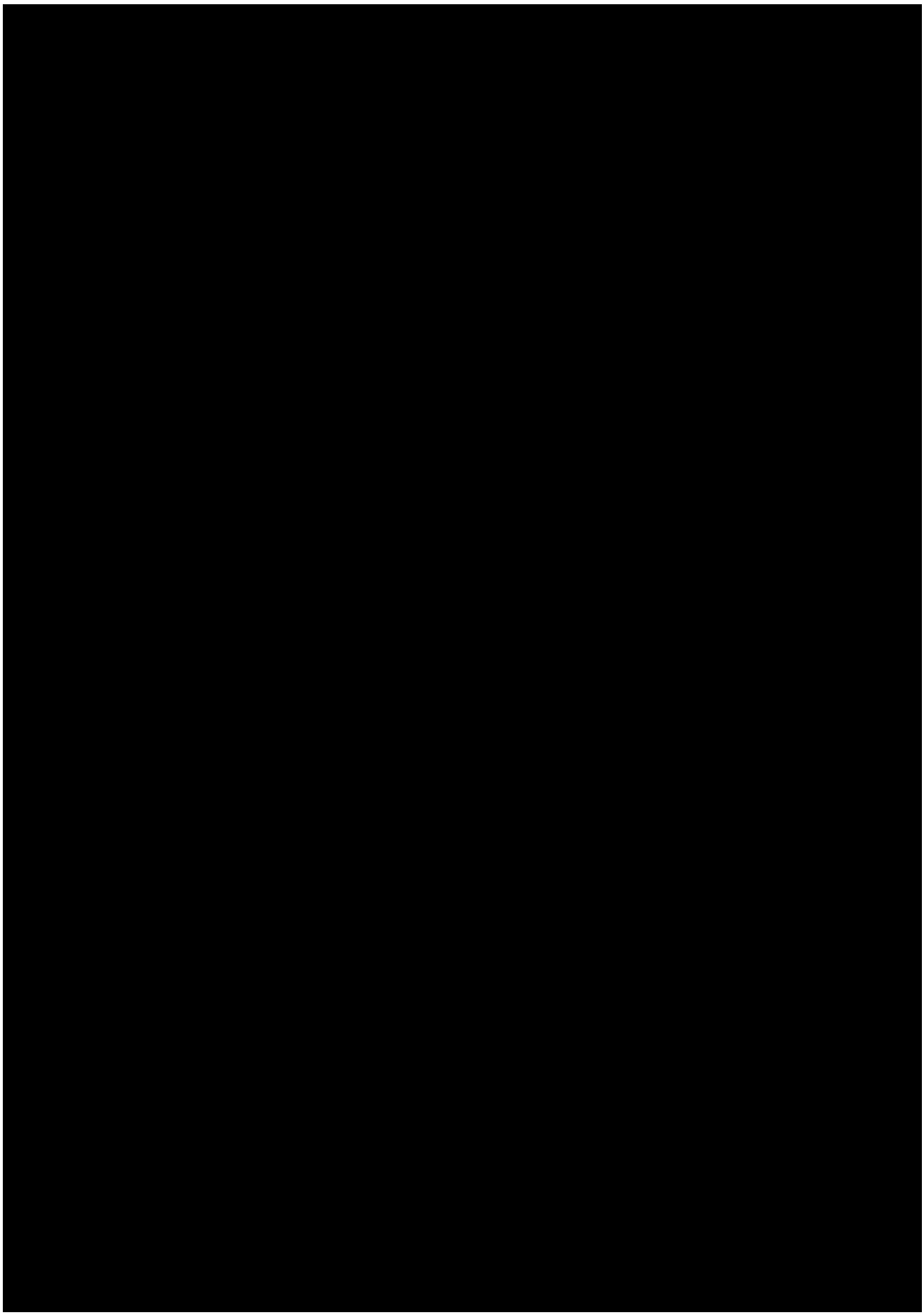
3 SPECIFIC OBLIGATIONS

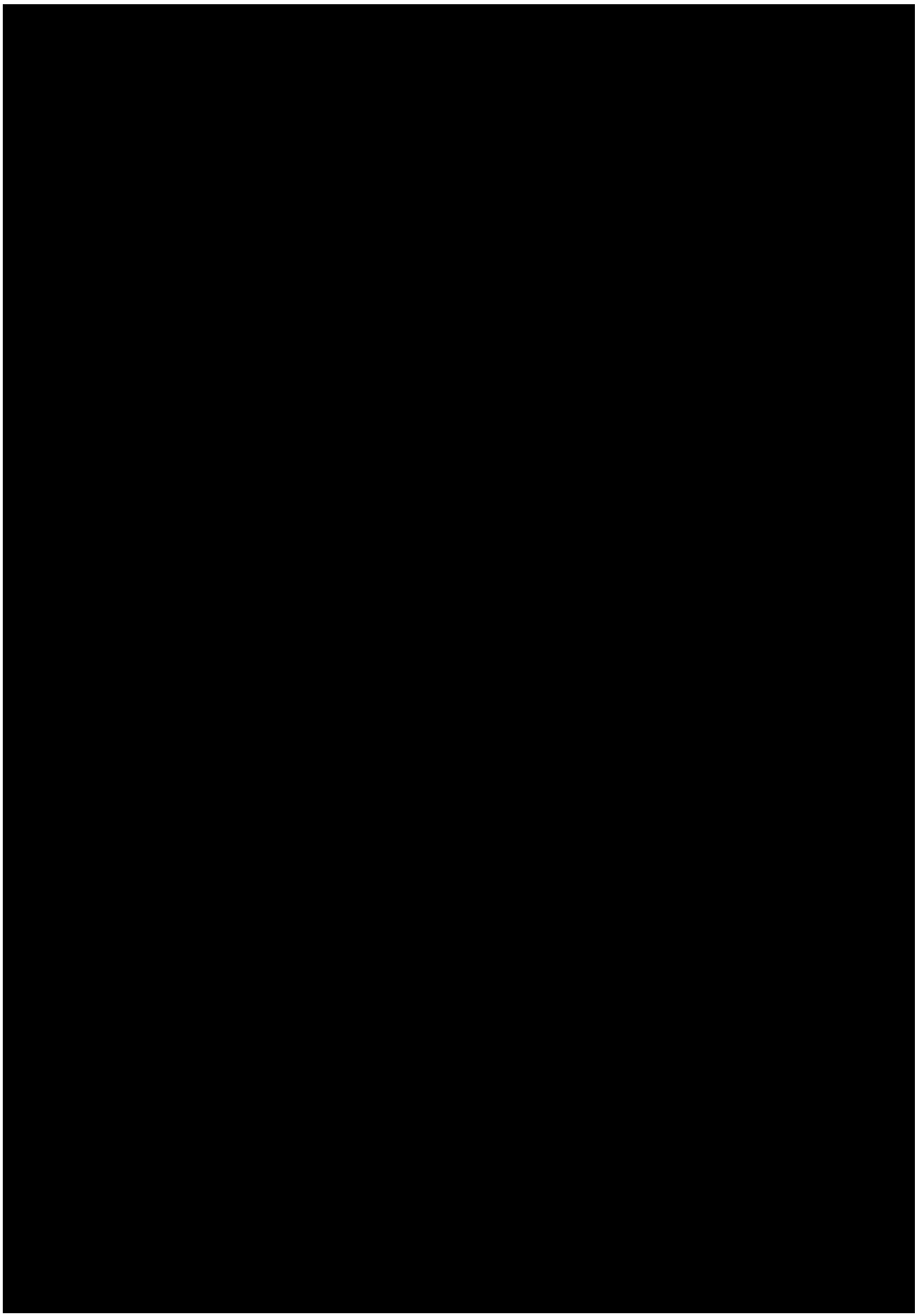
3.1 The Director shall, in relation to this Agreement perform the Director's Responsibilities identified as such in this Agreement the details of which are set out in the table below. References to milestones MS[nn] refer to milestones in the Outline Implementation Plan. Responsibilities shown as "SERVICE" continue throughout the Service period.

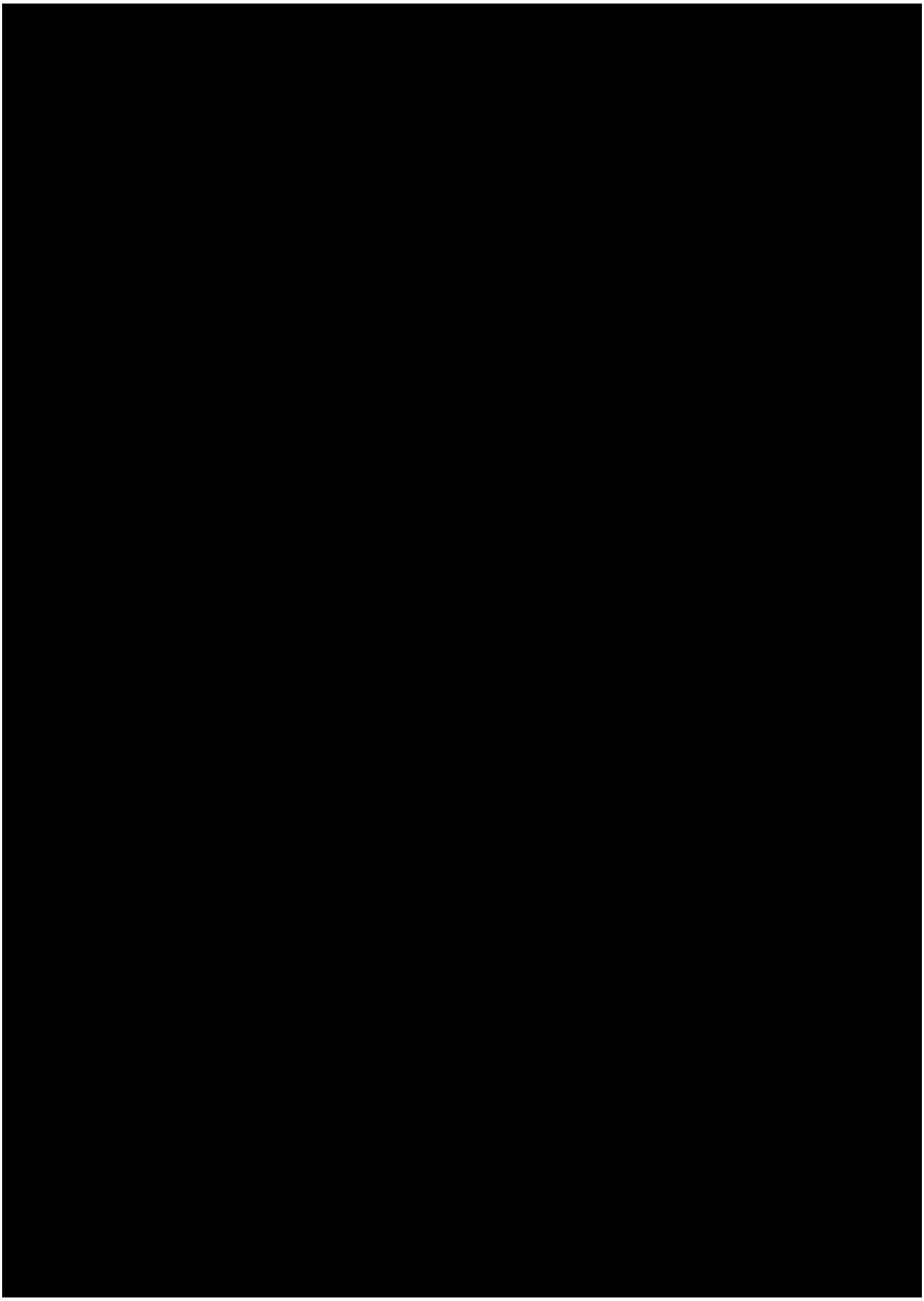










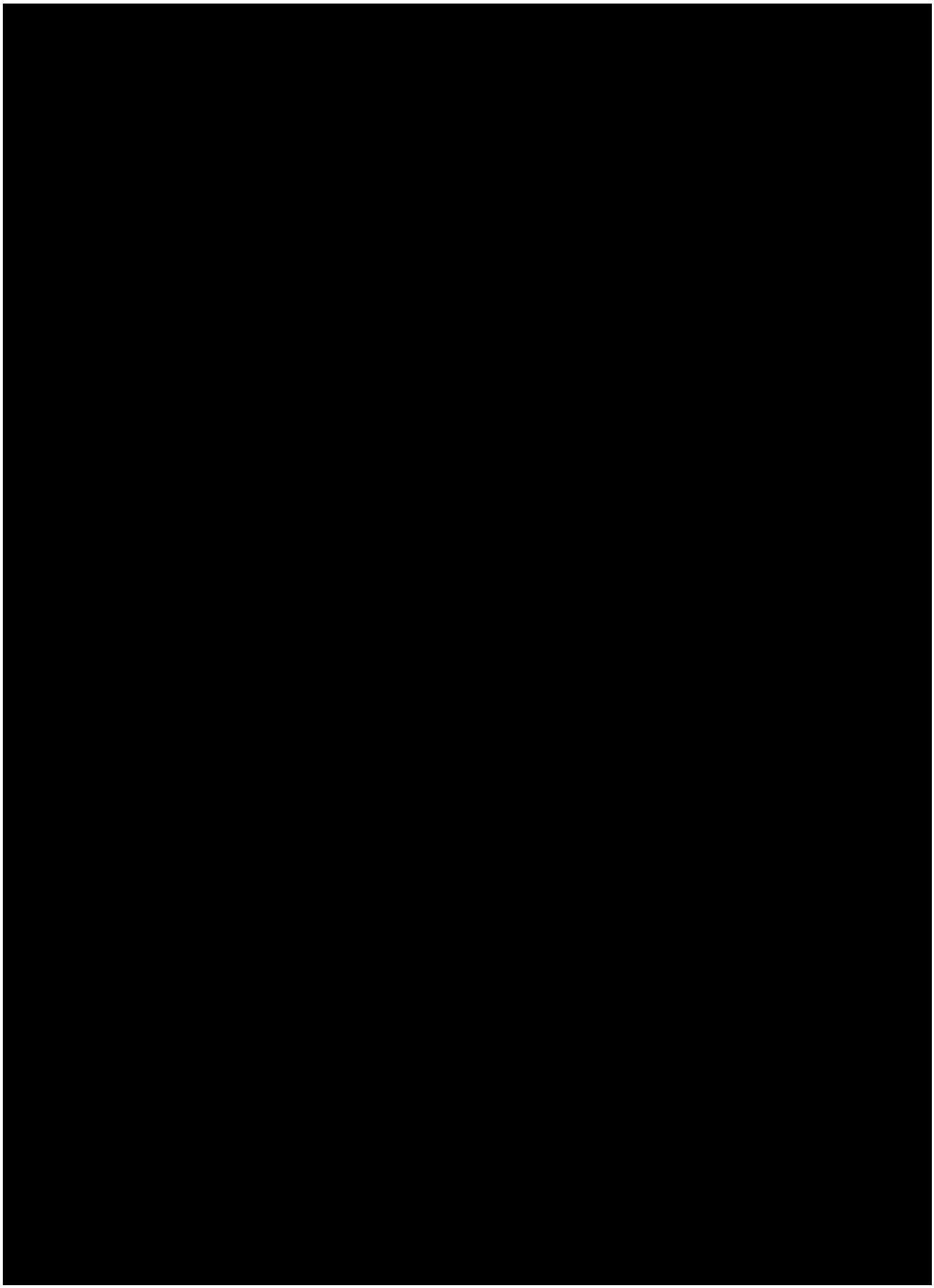


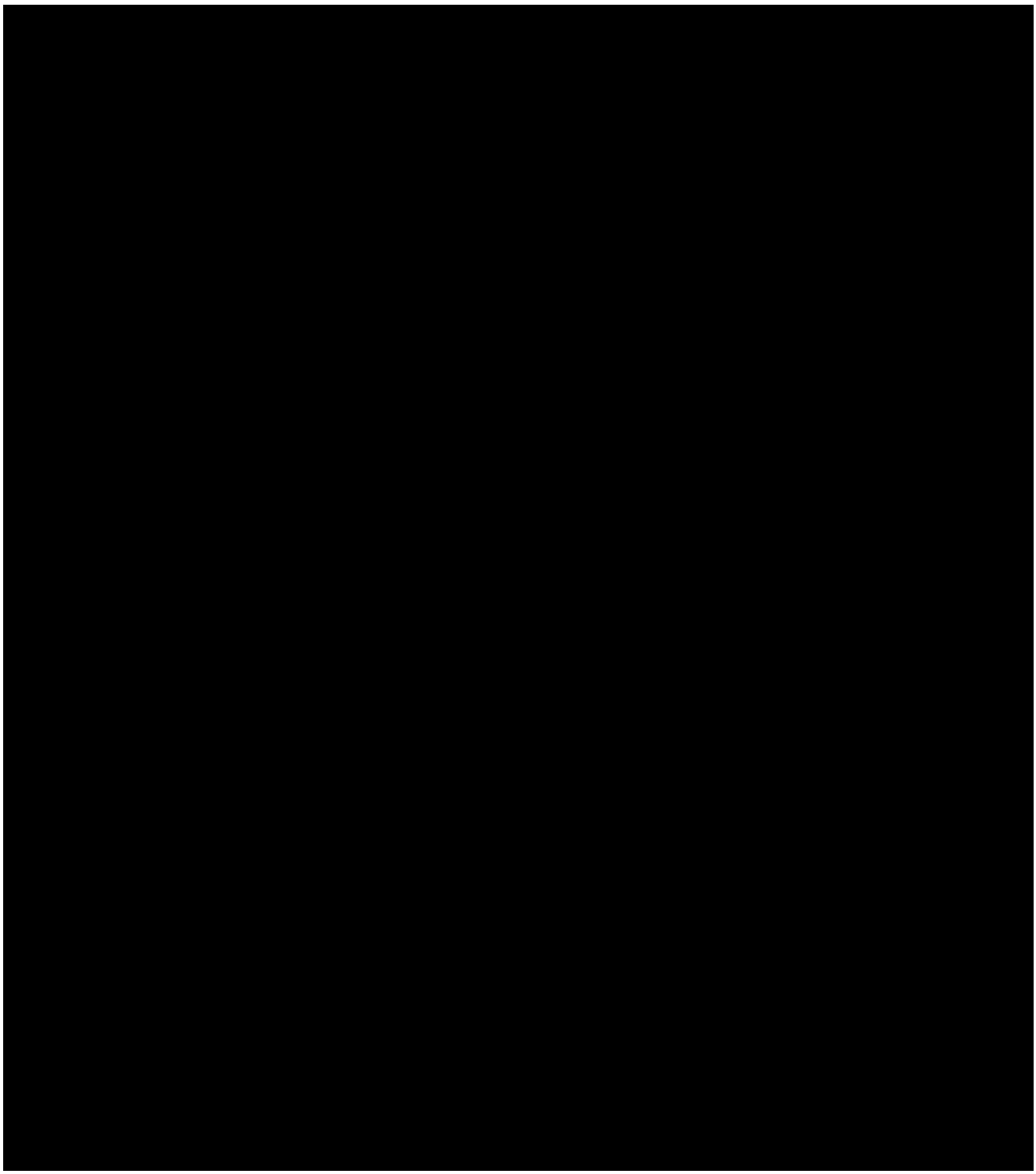
[redacted]

4 DEPENDENCIES ON RELEVANT THIRD-PARTY SUPPLIERS

4.1 The Director shall ensure that the Dependencies listed in the table below are added to the Collaboration Agreement and/or Operations Manual (as applicable) for the Relevant Third-Party Suppliers in accordance with the process and conditions set out therein no later than MS1.

[redacted]





INTRODUCTION

The contents of this Schedule 4.1 are extracted from the Suppliers' Final Tender. As the "quality" section of the Final Tender was structured as a set of responses to specific questions posed by the Director, those questions have been included within this Schedule 4.1, but that inclusion is for the purposes of context only and the questions themselves shall not be interpreted as forming part of the Service Delivery Solution.

In this Schedule 4.1 the Supplier details their solution to meet the Director's requirements set out across the Agreement, including Schedule 2.1 (Services Description), Schedule 2.2 (Performance Levels) and Schedule 2.4 (Security Management).

This takes the form of a number of sections that reflect the question responses submitted by the Supplier as part of their ISFT response. The questions are as follows:

No#	Title	Description
1	Proposed Future Target Operating Model	[redacted]
2	Take-on Operating Model & Transition Approach for Service Take-on	[redacted]
3	Transformation to Future Operating Model	[redacted]
4	Service Delivery	[redacted]
5	Proposed approach to Customer Migration to Digital	[redacted]

No#	Title	Description
		[redacted]
6	Proposed Solution for Change and Continuous Improvement	[redacted]
7	Proposed Solution for Collaborating, Delivering in Partnership and SIAM	[redacted]
8	Financial Crime Management and Compliance	[redacted]
9	Security	[redacted]
10	Social Value – Economic Sustainability Tackling	[redacted]

No#	Title	Description
	Economic Inequality: Increasing Supply Chain Resilience and Capacity	[redacted]
11	Social Value – Environmental Sustainability Fighting Climate Change: Effective Stewardship of the Environment	[redacted]
12	Social Value – Equal Opportunity – Reduction of Disability Employment Gap	[redacted]
13	Social Value – Social Sustainability Tackling Workforce Inequality: The Living Wage	[redacted]

SCHEDULE 4.2 - COMMERCIALLY SENSITIVE INFORMATION

Commercially Sensitive Information

No.	Date	Item(s)	Duration of Confidentiality
1	03/05/2023	All prices, costs, charges, rates and thresholds (other than the aggregate annual or total (for the Initial Term) value of the contract fixed charges) as set out in the Pricing Response Template or the Charging Model.	The Term plus seven years
2	03/05/2023	The processes and operation of the Digicare service as described in the response to Question 5 (Supplier IPR) in Schedule 4.1 (*Supplier Solution*).	The Term plus seven years
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			

SCHEDULE 4.3 - NOTIFIED KEY SUB-CONTRACTORS

Notified Key Sub-Contractors

1 In accordance with Clause 15.10 (*Appointment of Key Sub-contractors*), the Supplier is entitled to sub-contract its obligations under this Agreement to the Key Sub-contractors listed in the table below.

2 The Parties agree that they will update this Schedule periodically to record any Key Sub-contractors appointed by the Supplier with the consent of the Director after the Effective Date for the purposes of the delivery of the Services and to periodically review the status of existing Sub-contractors in accordance with the definition of a Key Sub-contractor.

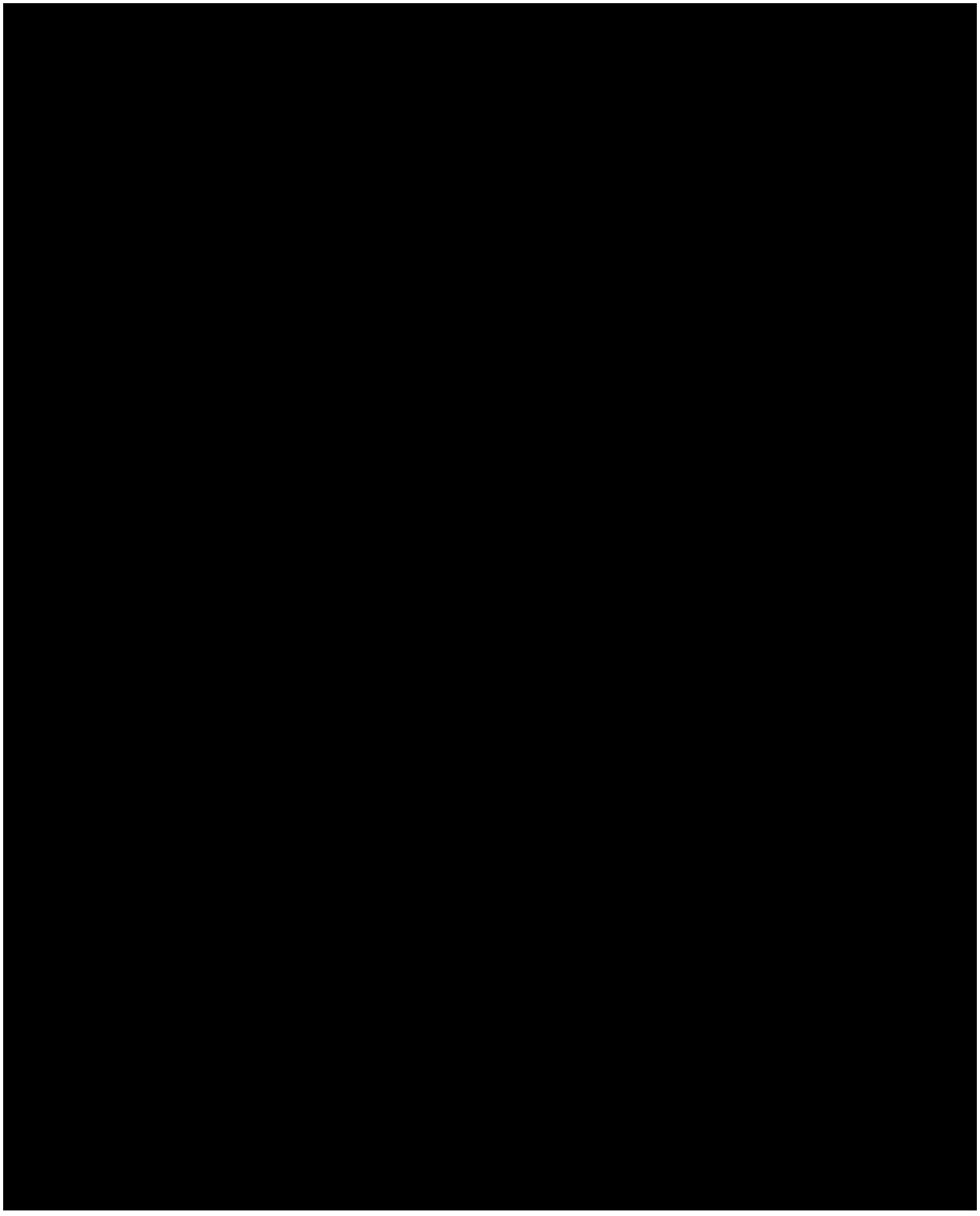
Key Sub-contractor name and address (if not the same as the registered office)	**Registered office and company number**	**Related product/ Service description**	**Key Sub-contract price expressed as a percentage of total projected Charges over the Term**	**Key role in delivery of the Services**	**Credit Rating Threshold**
None	N/A	N/A	N/A	N/A	N/A

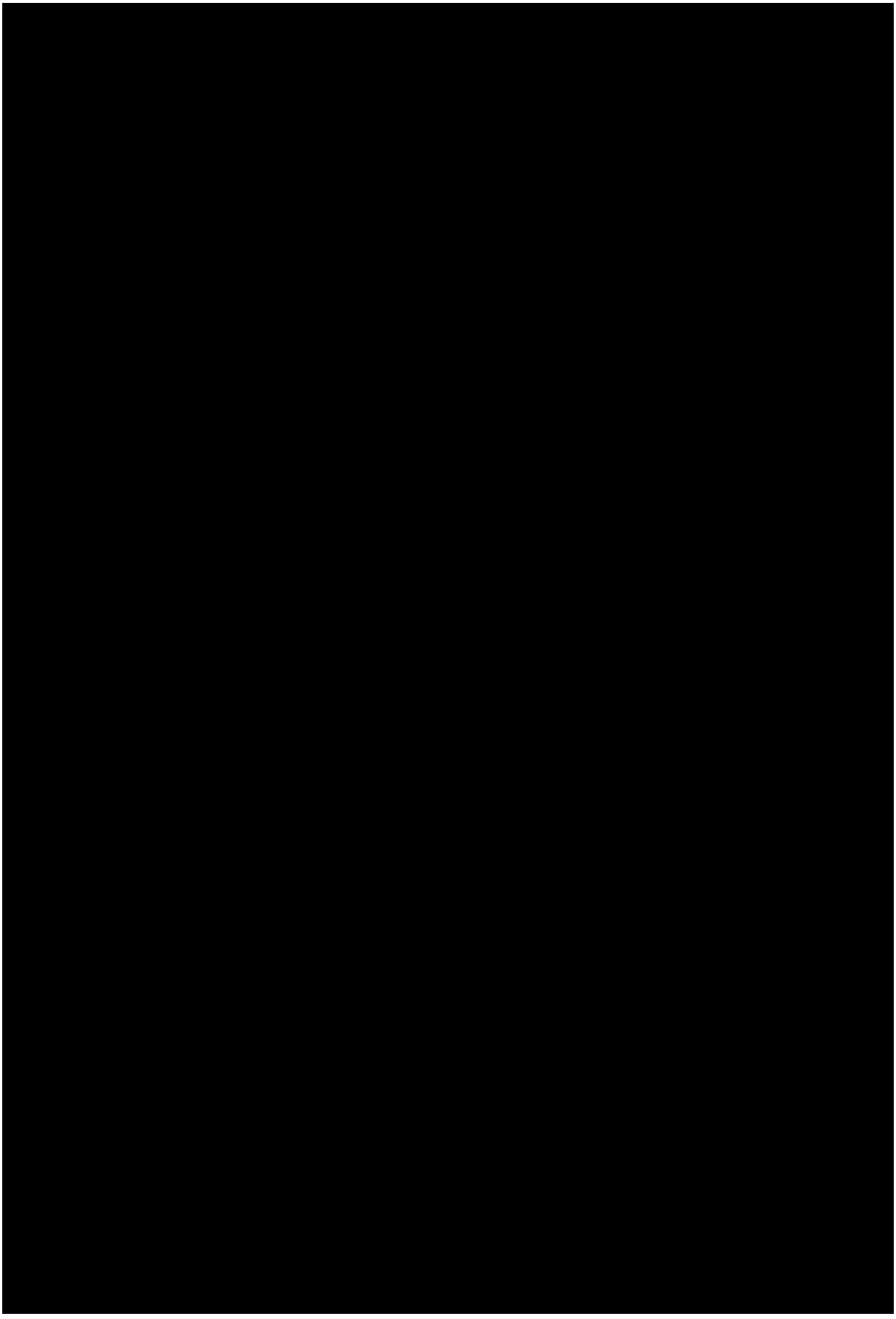
SCHEDULE 4.4 - THIRD PARTY CONTRACTS

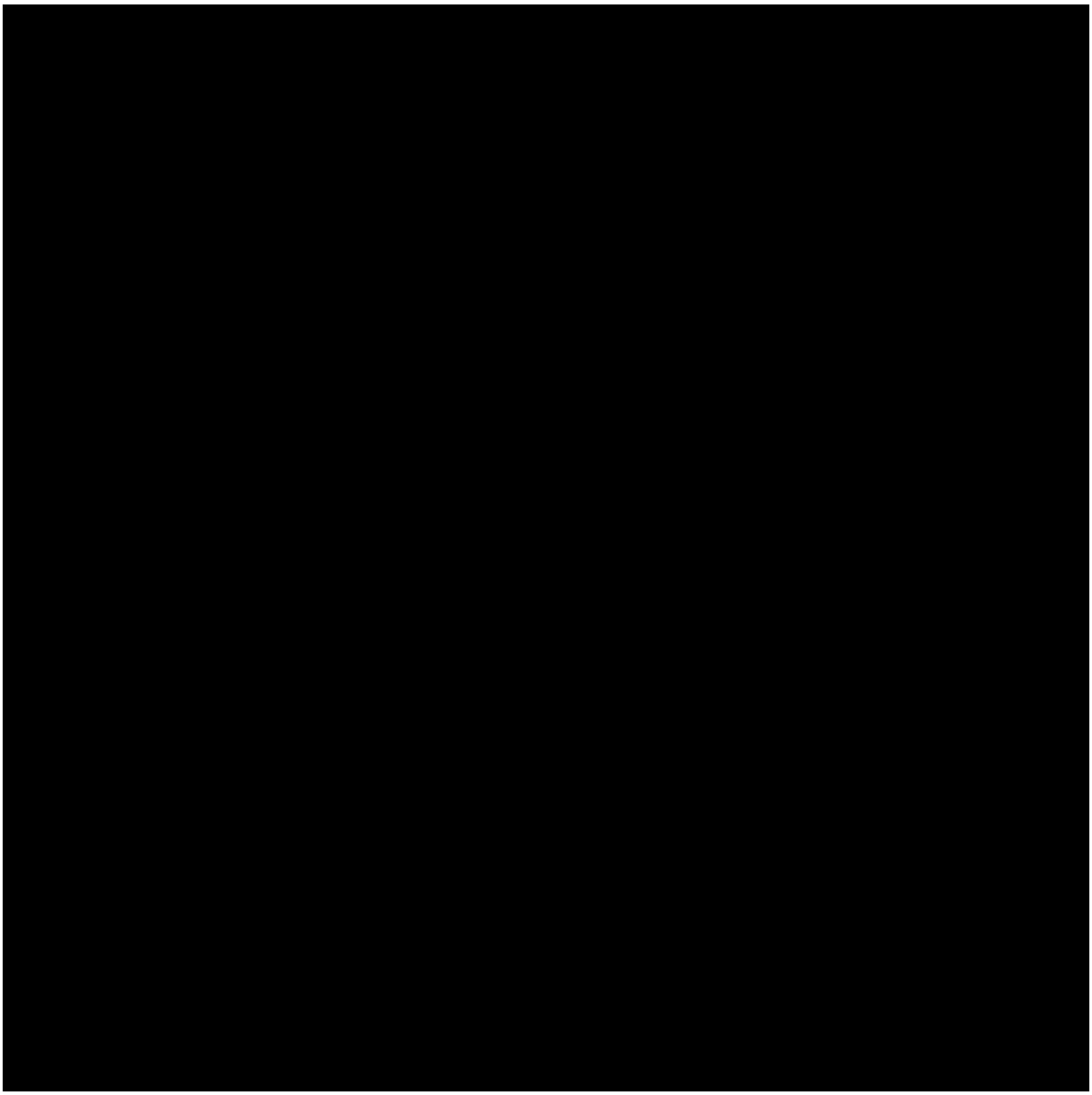
Third Party Contracts

1 The contracts listed in the table below constitute Third Party Contracts entered into exclusively for the purposes of delivering the Services.

2 The Supplier shall be entitled to update this Schedule in accordance with Clause 15.9 (*Appointment of Sub-contractors*).







SCHEDULE 5.1 - SOFTWARE

1 THE SOFTWARE

1.1 The Software below is licensed to the Director in accordance with Clauses 16 (*Intellectual Property Rights*) and 17 (*Transfer and Licences Granted by the Supplier*).

1.2 The Supplier shall promptly notify the Director of any updates to this Schedule and the Parties agree that they will update this Schedule regularly, and in any event no less than every three (3) Months from the Effective Date, to record any Supplier Software or Third Party Software subsequently licensed by the Supplier or third parties for the purposes of the delivery of the Services.

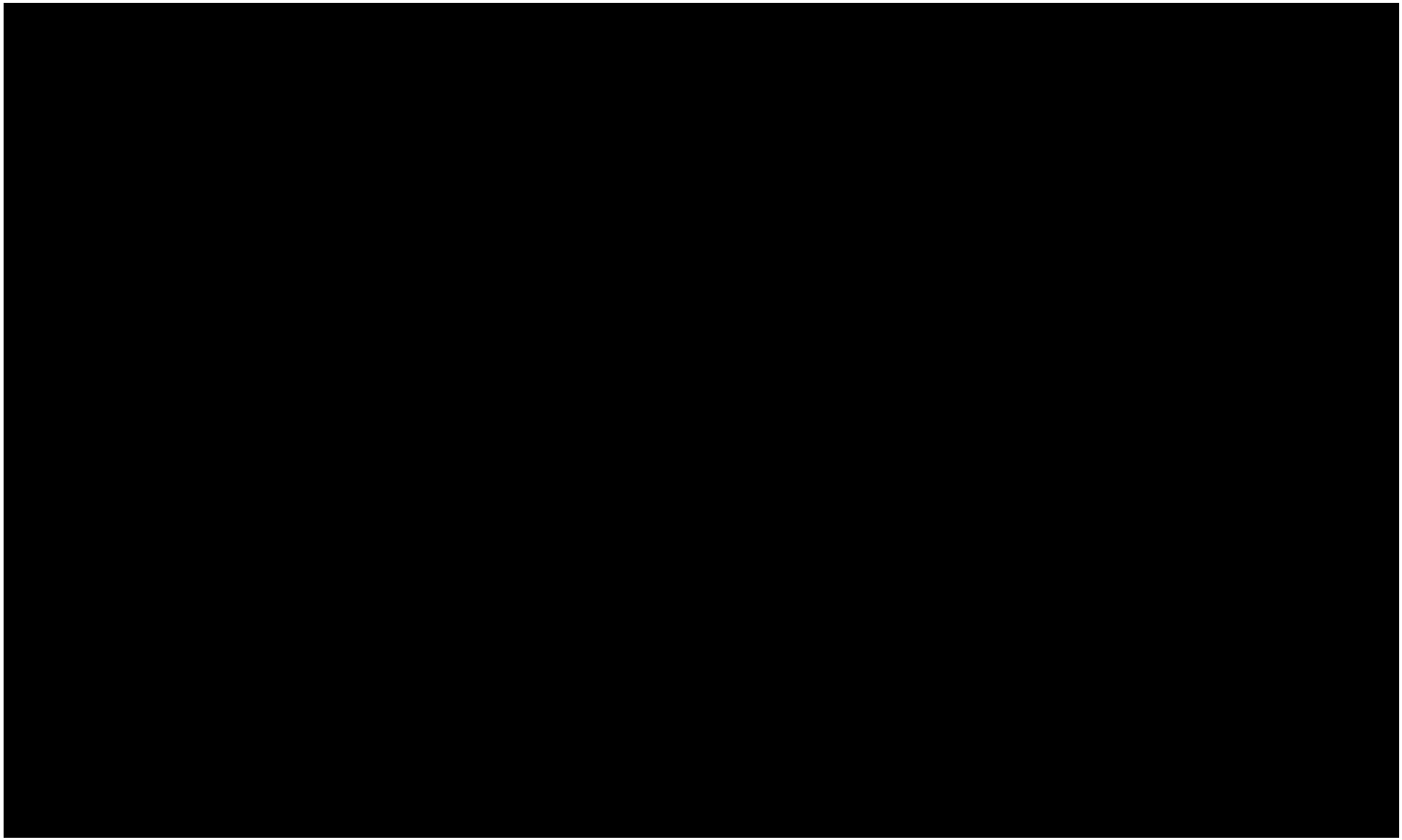
1.3 In addition to its obligation in respect of this Schedule, under Annex 3 of Schedule 8.4 (*Reports and Records Provisions*), the Supplier shall, if requested by the Director, report to the relevant governance body on such updates to this Schedule as required.

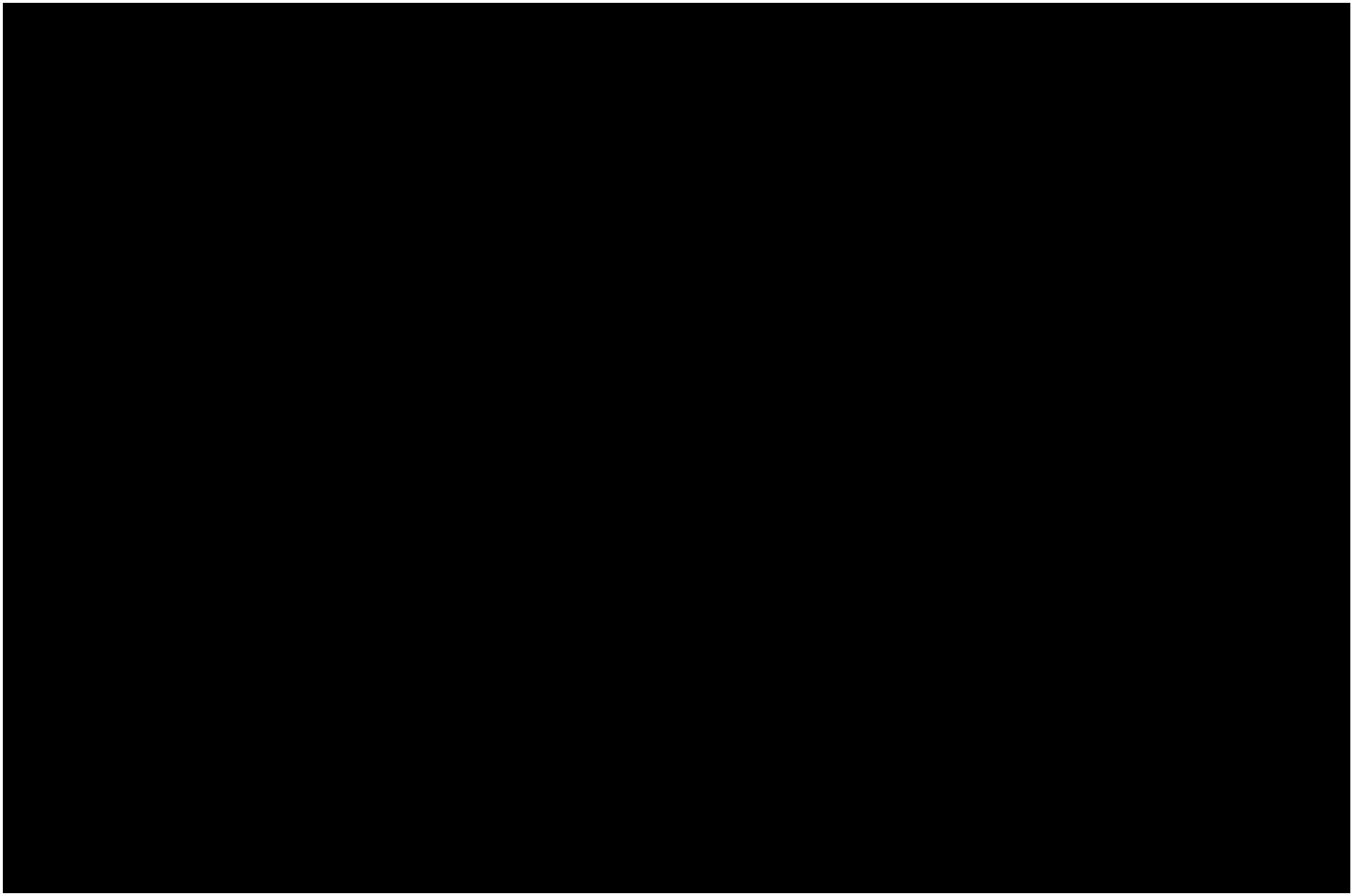
2 SUPPLIER SOFTWARE

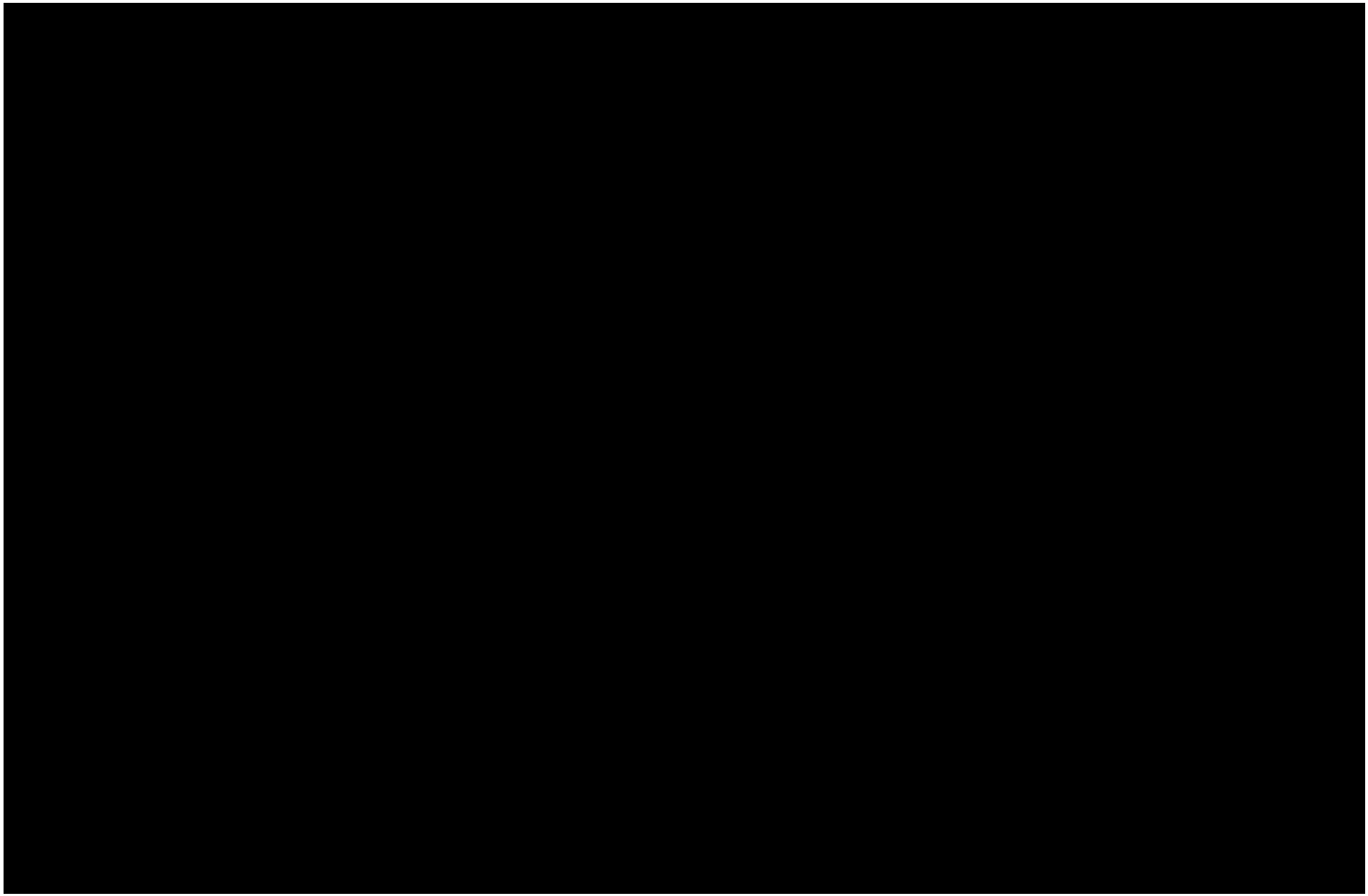
The Supplier Software includes the following items:

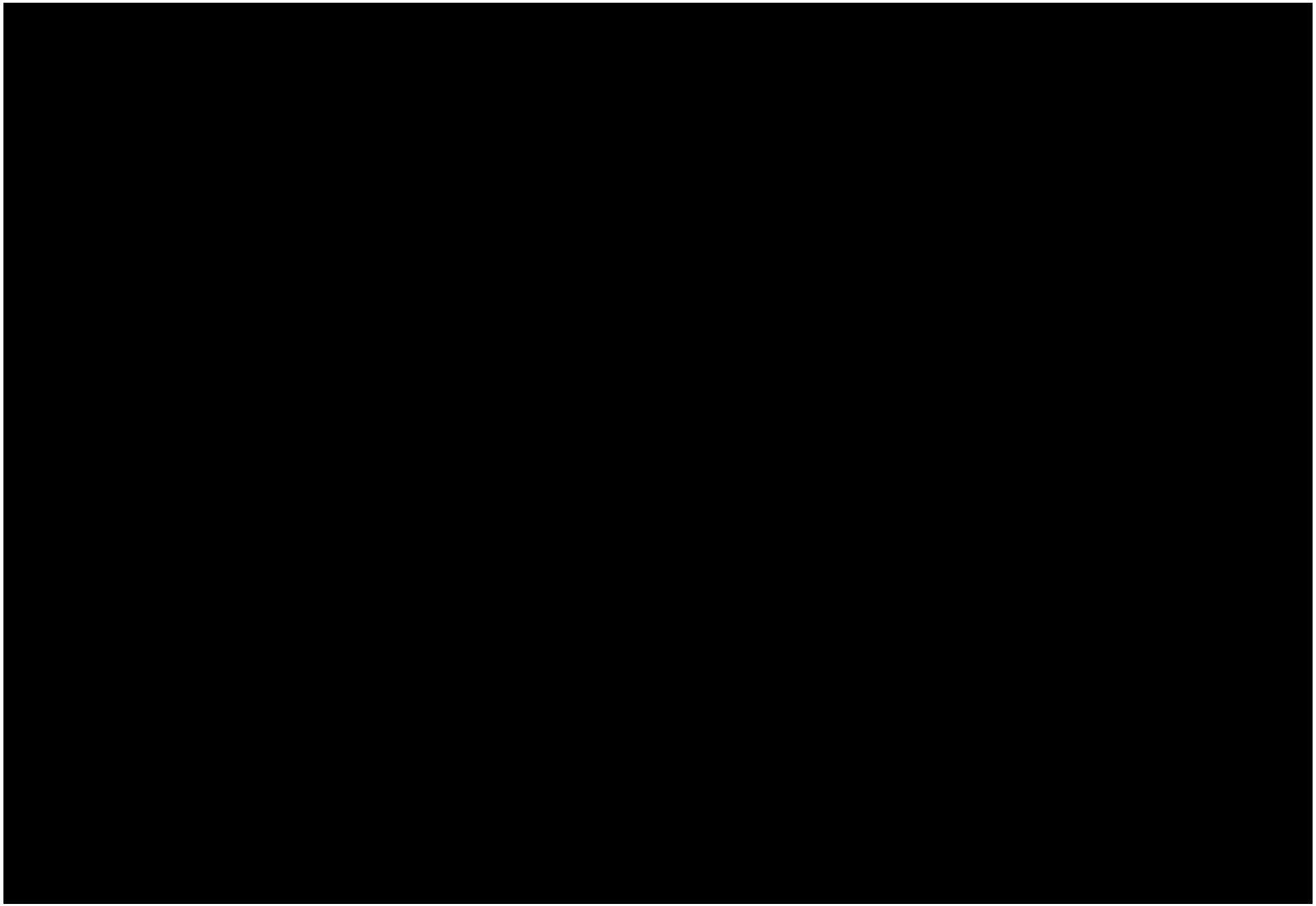
3 THIRD PARTY SOFTWARE

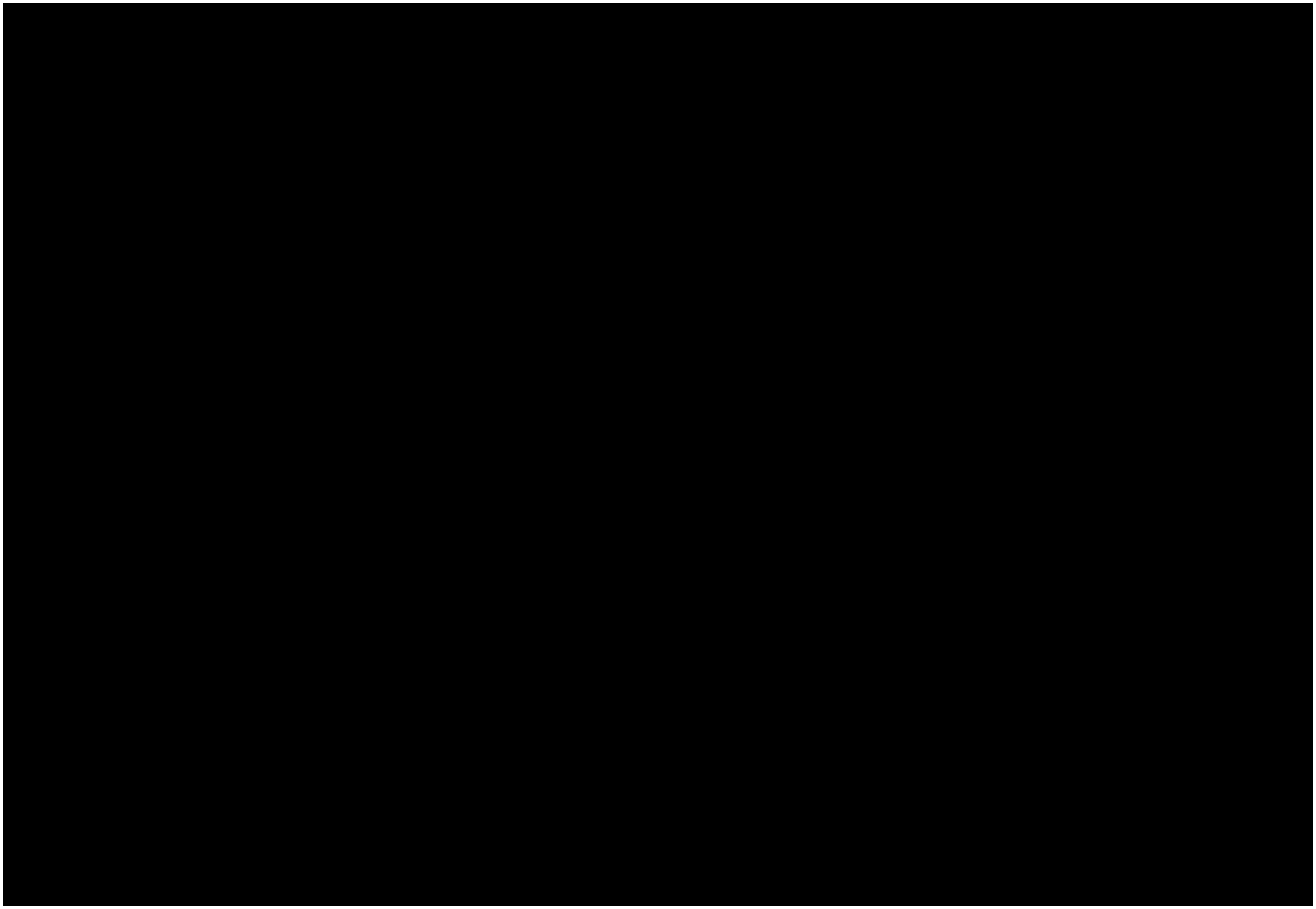
The Third Party Software shall include the following items:

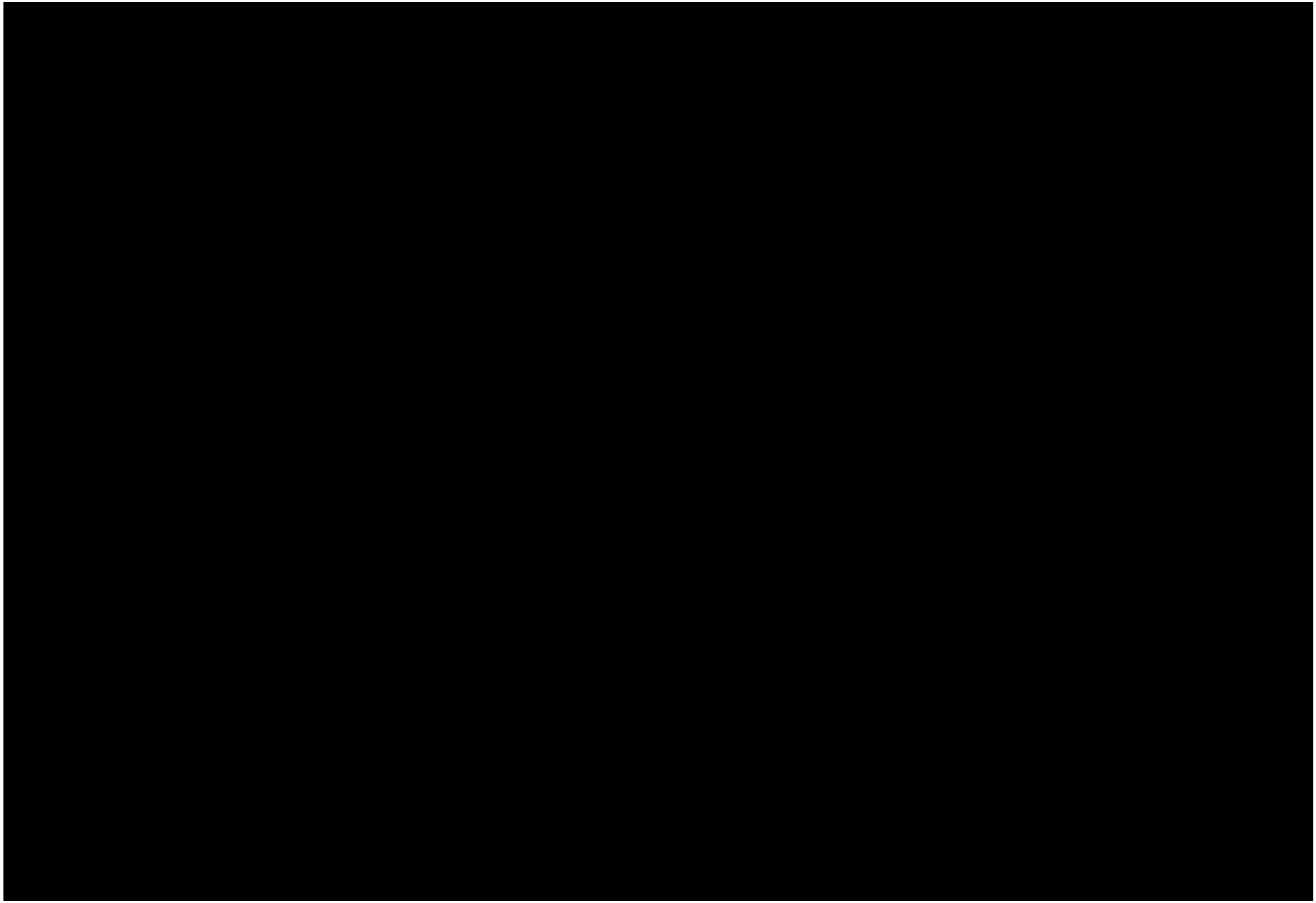


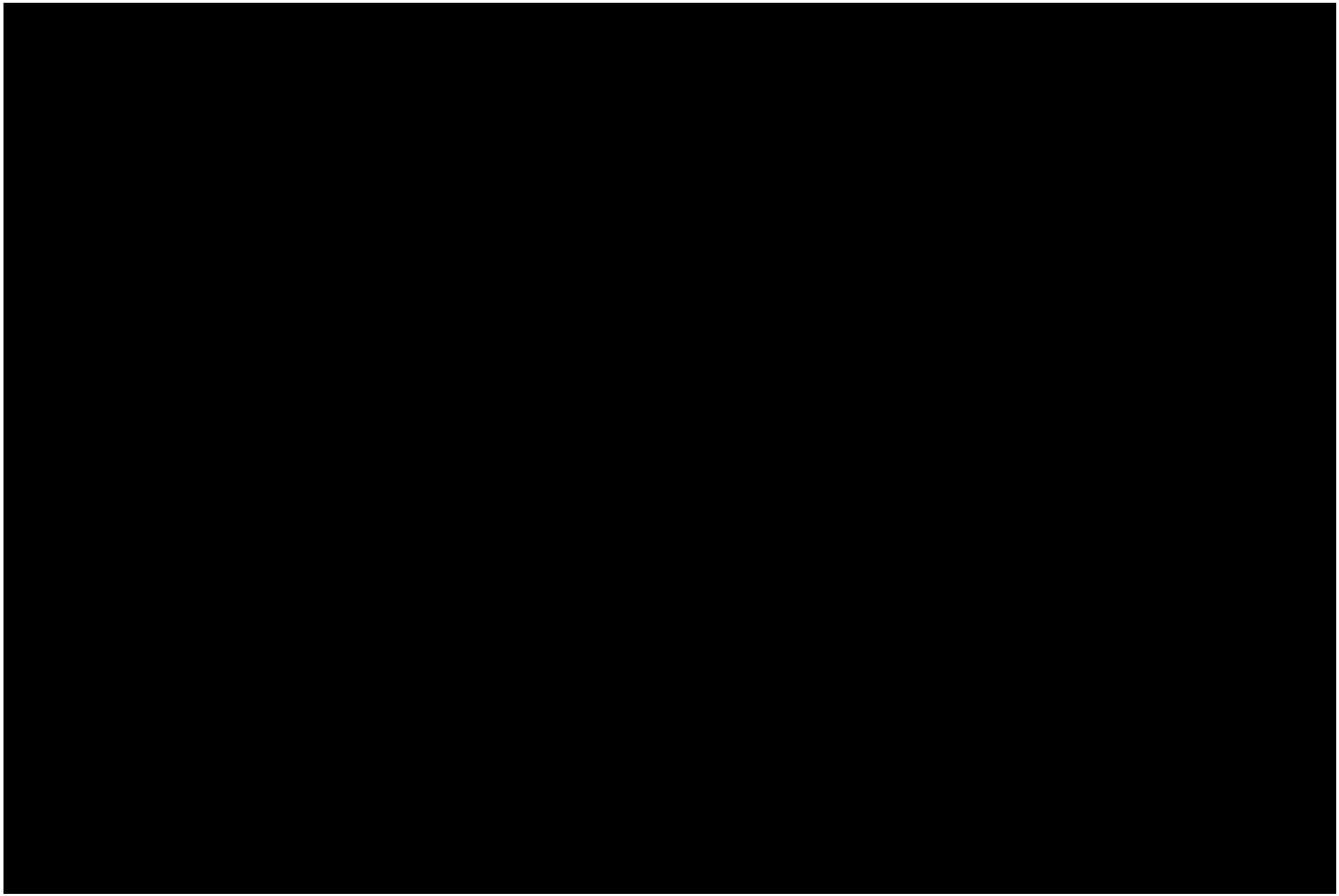


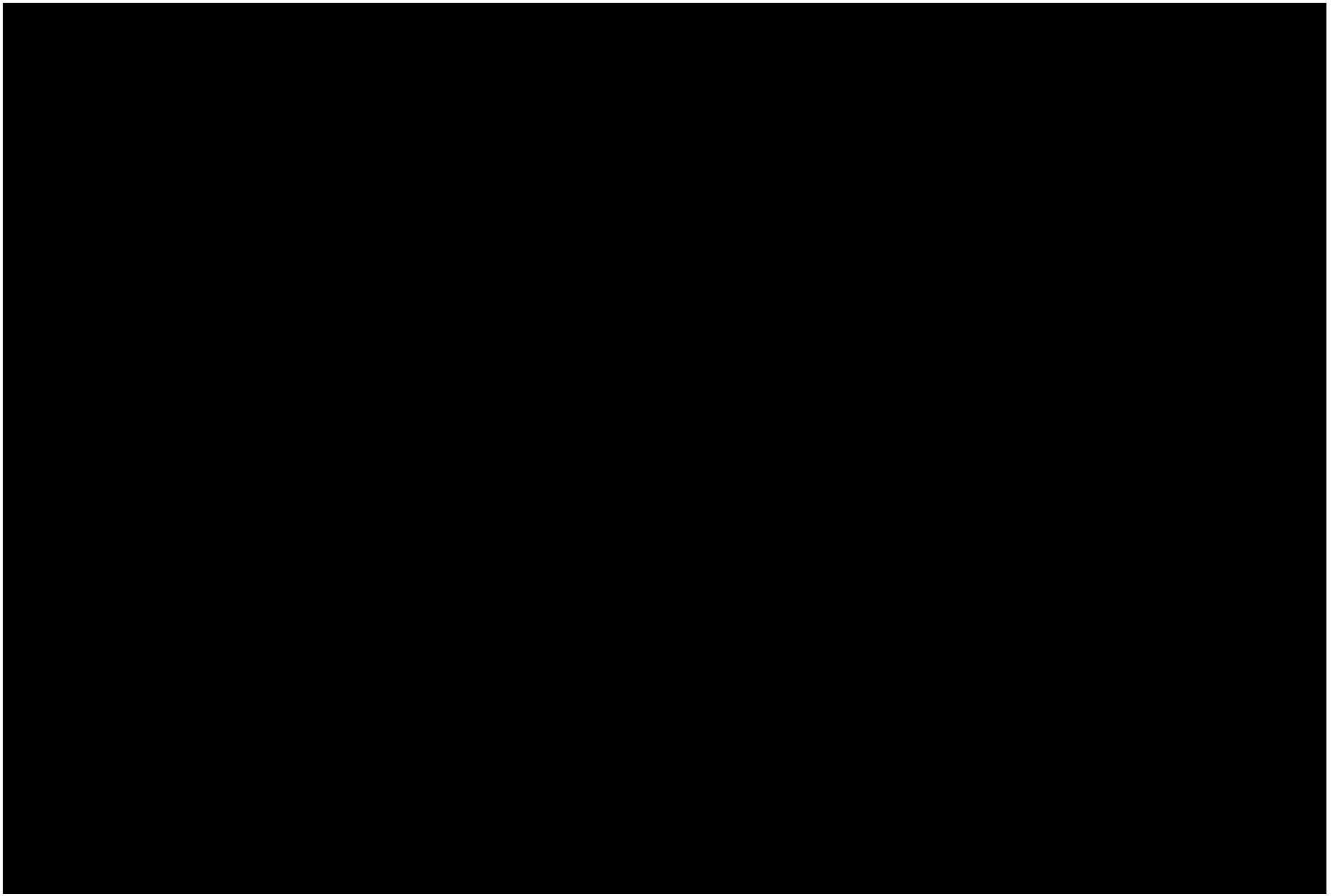


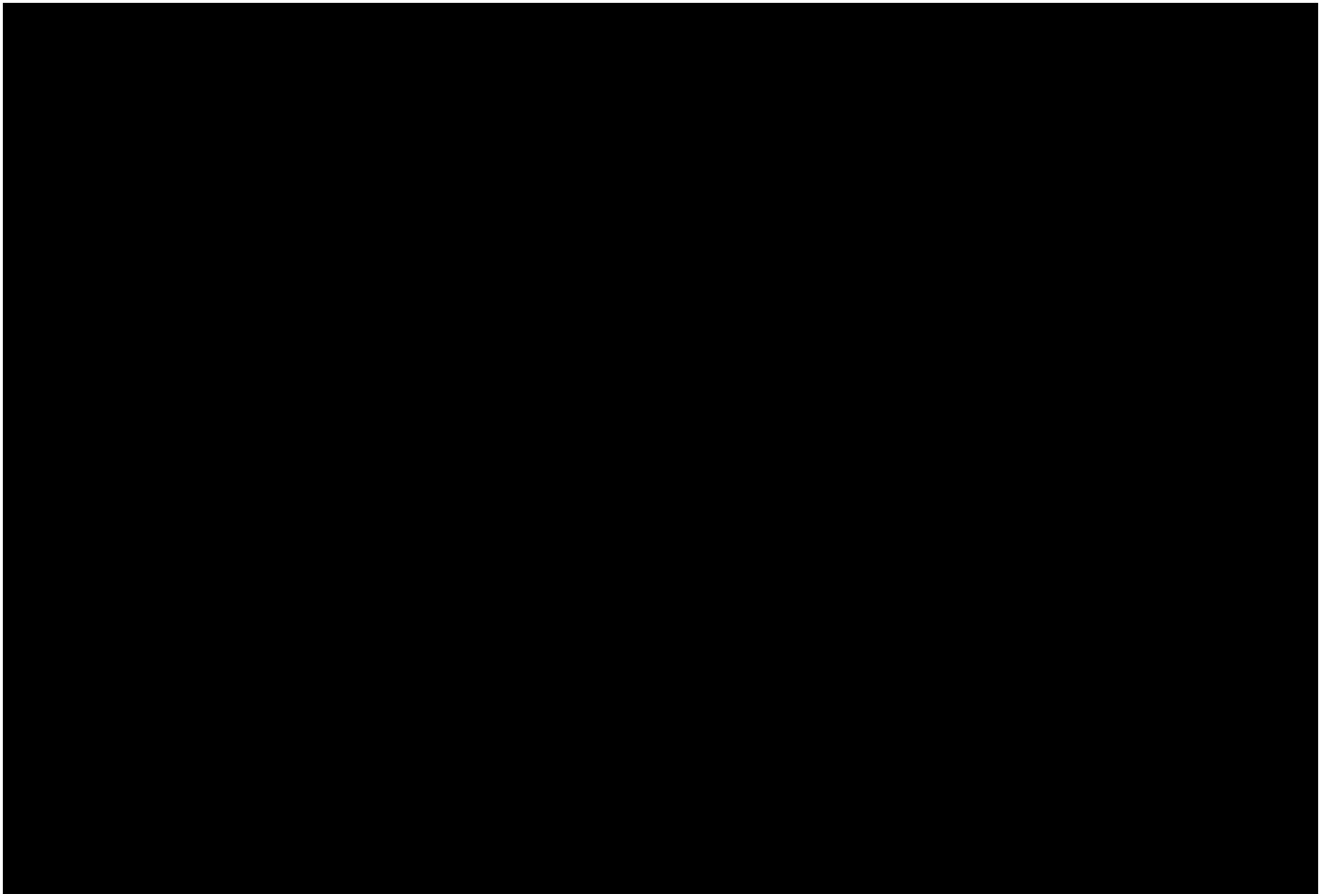












ANNEX 1: FORM OF LETTER RE SUB-LICENSING OF SUPPLIER SOFTWARE

[Supplier letterhead]

[insert Director name and address]

[Date]

Dear Sirs

LICENCES FOR SUPPLIER SOFTWARE

We refer to the agreement between us dated *[insert date]* in respect of *[brief summary of subject of the Agreement]* (the "**Agreement**"). Capitalised expressions used in this letter have the same meanings as in the Agreement.

In accordance with Clause 17.4.2 of the Agreement we confirm that:

1 the Director is licensed by the Supplier to use the [Supplier Software] and [Supplier Background IPRs] identified in the first column of the Appendix to this letter (the "**Appendix**") on the terms of the licences identified in the second column of the Appendix (the "**Licences**"); and

2 notwithstanding any provision to the contrary in the Licences, it is agreed that the Director may sub-license, assign and novate the [Supplier Software] and [Supplier Background IPRs] as referred to in Clause 17.4.2 of the Agreement.

Yours faithfully

Signed:

On behalf of [*name of the Supplier*]

ANNEX 2: FORM OF CONFIDENTIALITY UNDERTAKING

CONFIDENTIALITY AGREEMENT

THIS AGREEMENT is made on ***[date]*** 20

BETWEEN:

(1) **[*insert name*]** of [*insert address*] (the "**Sub-licensee**"); and

(2) **[*insert name*]** of [*insert address*] (the "**Supplier**" and together with the Supplier, the "**Parties**").

WHEREAS:

(A) The Director of Savings as agent of the Crown (the "**Director**") and the Supplier are party to a contract dated [*insert date*] (the "**Contract**") for the provision by the Supplier of [*insert brief description of services*] to the Director.

(B) The Director wishes to grant a sub-licence to the Sub-licensee in respect of certain software and intellectual property rights licensed to the Director pursuant to the Contract (the "**Sub-licence**").

(C) It is a requirement of the Contract that, before the Director grants such Sub-licence to the Sub-licensee, the Sub-licensee execute a confidentiality agreement in favour of the Supplier in or substantially in the form of this Agreement to protect the Confidential Information of the Supplier.

IT IS AGREED as follows:

1 Interpretation

1.1 In this Agreement, unless the context otherwise requires:

Confidential Information means:

(a) Information, including all personal data within the meaning of the Data Protection Act 2018, and however it is conveyed, provided by the Director to the Sub-licensee pursuant to or in connection with the Sub-licence that relates to:

(i) the Supplier; or

(ii) the operations, business, affairs, developments, intellectual property rights, trade secrets, know-how and/or personnel of the Supplier;

(b) the source code and the object code of the software sub-licensed to the Sub-licensee pursuant to the Sub-licence together with build information, relevant design and development information, technical specifications of all functionality including those not included in standard manuals (such as those that modify system performance and access levels), configuration details, test scripts, user manuals, operating manuals, process definitions and procedures, and all such other documentation supplied by the Supplier to the Director pursuant to or in connection with the Sub-licence;

(c) other Information provided by the Director pursuant to this Agreement to the Sub-licensee that is clearly designated as being confidential or equivalent or that ought reasonably to be considered to be confidential which comes (or has come) to the Sub-licensee's attention or into the Sub-licensee's possession in connection with the Sub-licence; and

(d) Information derived from any of the above,

but not including any Information that:

(a) was in the possession of the Sub-licensee without obligation of confidentiality prior to its disclosure by the Director;

(b) was already generally available and in the public domain at the time of disclosure otherwise than by a breach of this Agreement or breach of a duty of confidentiality; or

(c) was independently developed without access to the Information;

Information means all information of whatever nature, however conveyed and in whatever form, including in writing, orally, by demonstration, electronically and in a tangible, visual or machine-readable medium (including CD-ROM, magnetic and digital form); and

Sub-licence has the meaning given to that expression in recital (B) to this Agreement.

1.2 In this Agreement:

1.2.1 a reference to any gender includes a reference to other genders;

1.2.2 the singular includes the plural and vice versa;

1.2.3 the words "include" and cognate expressions shall be construed as if they were immediately followed by the words "without limitation";

1.2.4 references to any statutory provision include a reference to that provision as modified, replaced, amended and/or re-enacted from time to time (before or after the date of this Agreement) and any prior or subsequent subordinate legislation made under it;

1.2.5 headings are included for ease of reference only and shall not affect the interpretation or construction of this Agreement; and

1.2.6 references to Clauses are to Clauses of this Agreement.

2 Confidentiality Obligations

2.1 In consideration of the Director entering into the Sub-licence, the Sub-licensee shall:

2.1.1 treat all Confidential Information as secret and confidential;

2.1.2 have in place and maintain proper security measures and procedures to protect the confidentiality of the Confidential Information (having regard to its form and nature);

2.1.3 not disclose or permit the disclosure of any of the Confidential Information to any other person without obtaining the prior written consent of the Supplier or except as expressly set out in this Agreement;

2.1.4 not transfer any of the Confidential Information outside the United Kingdom;

2.1.5 not use or exploit any of the Confidential Information for any purpose whatsoever other than as permitted under the Sub-licence;

2.1.6 immediately notify the Supplier in writing if it suspects or becomes aware of any unauthorised access, copying, use or disclosure in any form of any of the Confidential Information; and

2.1.7 upon the expiry or termination of the Sub-licence:

(a) destroy or return to the Supplier all documents and other tangible materials that contain any of the Confidential Information;

(b) ensure, so far as reasonably practicable, that all Confidential Information held in electronic, digital or other machine-readable form ceases to be readily accessible (other than by the information technology staff of the Sub-licensee) from any computer, word processor, voicemail system or any other device; and

(c) make no further use of any Confidential Information.

3 Permitted Disclosures

3.1 The Sub-licensee may disclose Confidential Information to those of its directors, officers, employees, consultants and professional advisers who:

3.1.1 reasonably need to receive the Confidential Information in connection with the Sub-licence; and

3.1.2 have been informed by the Sub-licensee of the confidential nature of the Confidential Information; and

3.1.3 have agreed to terms similar to those in this Agreement.

3.2 The Sub-licensee shall be entitled to disclose Confidential Information to the extent that it is required to do so by applicable law or by order of a court or other public body that has jurisdiction over the Sub-licensee.

3.3 Before making a disclosure pursuant to Clause3.2, the Sub-licensee shall, if the circumstances permit:

3.3.1 notify the Supplier in writing of the proposed disclosure as soon as possible (and if possible before the court or other public body orders the disclosure of the Confidential Information); and

3.3.2 ask the court or other public body to treat the Confidential Information as confidential.

4 General

4.1 The Sub-licensee acknowledges and agrees that all property, including intellectual property rights, in Confidential Information disclosed to it by the Supplier shall remain with and be vested in the Supplier.

4.2 This Agreement does not include, expressly or by implication, any representations, warranties or other obligations:

4.2.1 to grant the Sub-licensee any licence or rights other than as may be expressly stated in the Sub-licence;

4.2.2 to require the Supplier to disclose, continue disclosing or update any Confidential Information; or

4.2.3 as to the accuracy, efficacy, completeness, capabilities, safety or any other qualities whatsoever of any Information or materials provided pursuant to or in anticipation of the Sub-licence.

4.3 The rights, powers and remedies provided in this Agreement are cumulative and not exclusive of any rights, powers or remedies provided by law. No failure or delay by either Party to exercise any right, power or remedy will operate as a waiver of it nor will any partial exercise preclude any further exercise of the same, or of some other right, power or remedy.

4.4 Without prejudice to any other rights or remedies that the Supplier may have, the Sub-licensee acknowledges and agrees that damages alone may not be an adequate remedy for any breach by the Sub-licensee of any of the provisions of this Agreement. Accordingly, the Sub-licensee acknowledges that the Supplier shall be entitled to the remedies of injunction and specific performance as well as

any other equitable relief for any threatened or actual breach of this Agreement and/or breach of confidence and that no proof of special damages shall be necessary for the enforcement of such remedies.

4.5 The maximum liability of the Sub-licensee to the Supplier for any breach of this Agreement shall be limited to ten million pounds (£10,000,000).

4.6 For the purposes of the Contracts (Rights of Third Parties) Act 1999 no one other than the Parties has the right to enforce the terms of this Agreement.

4.7 Each Party shall be responsible for all costs incurred by it or on its behalf in connection with this Agreement.

4.8 This Agreement may be executed in any number of counterparts and by the Parties on separate counterparts, but shall not be effective until each Party has executed at least one counterpart. Each counterpart shall constitute an original of this Agreement, but all the counterparts shall together constitute but one and the same instrument.

5 Notices

5.1 Any notice to be given under this Agreement (each a "**Notice**") shall be given in writing and shall be delivered by hand and shall be deemed to have been duly given at the time of delivery provided that such Notice is sent to the relevant physical address, and expressly marked for the attention of the relevant individual, set out in Clause5.2.

5.2 Any Notice:

5.2.1 if to be given to the Supplier shall be sent to:

[*Address*]

Attention: [*Contact name and/or position, e.g. "The Finance Director"*]

5.2.2 if to be given to the Sub-licensee shall be sent to:

[*Name of Organisation*]

[*Address*]

Attention: [ ]

6 Governing law

6.1 This Agreement shall be governed by, and construed in accordance with, English law and any matter claim or dispute arising out of or in connection with this Agreement whether contractual or non-contractual, shall be governed by and determined in accordance with English law.

6.2 Each Party hereby irrevocably submits to the exclusive jurisdiction of the English courts in respect of any claim or dispute arising out of or in connection with this Agreement.

IN WITNESS of the above this Agreement has been signed by the duly authorised representatives of the Parties on the date which appears at the head of the first page.

For and on behalf of [*name of Supplier*]

Signature: Date:

Name: Position:

For and on behalf of [*name of Sub-licensee*]

Signature: Date:

Name: Position:

SCHEDULE 5.2 – TRADE MARK LICENCE TERMS

1 DEFINITIONS

1.1 The definitions in this Paragraph 1 shall apply for the purposes of this Schedule:

1.1.1 "**Brand Guidelines**" means the document issued by the Director from time to time setting out how the Trade Marks, logos and other communications material must be presented and structured to support the NS&I brand (the Supplier shall be notified in writing of any updates to this document);

1.1.2 "**Territory**" means the United Kingdom; and

1.1.3 "**Trade Marks**" means the registered trade marks listed in Annex 1 of Schedule (Trade Mark Licence Terms), any unregistered trade marks explicitly agreed for use by the Supplier in the provision of the Services by the Director in writing and any application which may be made for a trade mark which is identical with or similar to any of the words or devices which is the subject of any of the Trade Marks and "the Trade Mark" means any one of the Trade Marks relevant in that context.

2 USE OF TRADE MARKS

2.1 The Supplier shall, in providing the Services use best endeavours, at all times, to maintain and enhance goodwill in the Director's business using the Trade Marks.

2.2 The Supplier shall use the Trade Marks only in relation to Services, and promotional material relating to such Services, which comply with the Brand Guidelines.

2.3 The Supplier shall use the Trade Marks only in relation to the Services and promotional material and content relating to such Services in accordance with the Brand Guidelines.

2.4 The Supplier shall make any changes requested by the Director relating to its use of the Trade Marks including providing the Services in accordance with amended Brand Guidelines and withdrawing Services which the Director states, in its absolute discretion, do not comply with the Brand Guidelines.

3 TREATMENT OF TRADE MARKS

3.1 The Director shall be responsible for maintaining and renewing any registrations for the Trade Marks (as applicable), for the prosecution of any new applications and the conduct of any opposition or rectification action which relates to any of the Trade Marks. The Director's decision on whether or not to prosecute any application or other action in relation to the Trade Marks shall be final and shall not reduce any obligation on the Supplier to provide the Services.

3.2 The Supplier will not do anything to prejudice or to endanger the value or validity of any of the Trade Marks and will not use the Trade Marks other than in relation to Services that conform to the Brand Guidelines. In particular, the Supplier shall not use the Trade Marks in any way which would allow them to become generic, lose their distinctiveness, become liable to mislead the public, or be materially detrimental to or inconsistent with the good name, goodwill, reputation and image of the Director.

3.3 The Supplier shall, as requested by the Director, include in its advertisements and other promotional material for the Services words or other material making it clear that any of the Trade Marks are (where applicable) registered trade marks and that such Trade Marks are the property of the Director.

3.4 No trade mark other than the Trade Marks shall be used by the Supplier in relation to the Services without the prior written permission of the Director. The conditions of use of any such trade mark are to be agreed between the Parties, and the Director's decision as to use of such marks shall be final. If the Director gives consent, the trade mark that is not one of the Trade Marks shall be presented

separately from the Trade Marks so that each appears to be a trade mark in its own right distinct from the other Trade Mark.

3.5 The Supplier shall not use the Trade Marks in proximity to any third party trade mark or on the same webpage as any third party trade mark without the express written consent of the Director.

3.6 The Supplier recognises the Director's title to the Trade Marks and that all goodwill generated by its use of the Trade Marks will inure to the benefit of the Director. The Supplier acknowledges that it shall not, by virtue of this Agreement, obtain or claim any right, title or interest in or to the Trade Marks except the rights of use as are specifically set out in this Licence.

3.7 The Supplier shall not use any of the Trade Marks as part of its corporate or business name, trading style or part of the name of any entity connected with it without the prior written consent of the Director.

4 TRADE MARK PROCEEDINGS AGAINST THIRD PARTIES

4.1 The Supplier shall as soon as possible notify the Director of:

4.1.1 all possible infringements of the Trade Marks or any relevant passing off or unfair competition;

4.1.2 any application to register trade marks which may conflict or be confused with any of the Trade Marks; or

4.1.3 any claim by or notification of intention to make a claim from a third party which may come to its attention,

and the Director shall take such measures as it considers appropriate in respect of any incidents of infringement, passing off or unfair competition, or to prevent the registration of such trade marks, and the Supplier shall at the request and the expense of the Director provide all reasonable assistance in relation to such measures.

4.2 The Director shall have the exclusive right to take and conduct action against third parties in respect of the Trade Marks. For the avoidance of doubt, the Supplier waives its rights under s.30(2) and s.30(3) of the Trade Marks Act 1994.

ANNEX 1

THE TRADE MARKS

1 REGISTERED TRADE MARKS

Country	Mark	Registration No.	Class(es)	Date granted
United Kingdom	Chestnut logo *(Figurative – series of 4)*	2450787	9, 16, 35, 36, 41	21 Sept 2007
United Kingdom	ERNIE	2450620	9, 16, 35, 36, 41	29 Feb 2008
United Kingdom	National Savings	2450778	9, 16, 35, 41	28 Mar 2008
United Kingdom	National Savings	2450622	16	28 Mar 2008
United Kingdom	National Savings	1366688	36	26 Oct 1990
United Kingdom	National Savings & Investments	2450609	9, 16, 25, 35, 36, 41	04 Apr 2008
United Kingdom	National Savings & Investments	2450617	9, 16, 25, 35, 36, 41	04 Apr 2008
United Kingdom	ns&i logo *(Figurative – series of 4)*	2450782	9, 16, 35, 36, 41	07 Dec 2007
United Kingdom	NATIONAL SAVINGS AND INVESTMENTS	2450608	9, 16, 25, 35, 41	28 Mar 2008
United Kingdom	National Savings and Investments	2450610	9, 16, 18, 25, 35, 36, 41	04 Apr 2008
United Kingdom	NATIONAL SAVINGS AND INVESTMENTS	2293327	36	23 Aug 2002
United Kingdom	ns and i	2450615	9, 16, 35, 36, 41	29 Feb 2008
United Kingdom	NS and I	2450776	9, 16, 35, 36, 41	22 Feb 2008
United Kingdom	NS&I	2450616	9, 16, 35, 36, 41	29 Feb 2008
United Kingdom	ns&i	2450611	9, 16, 25, 35, 36, 41	29 Feb 2008

Country	Mark	Registration No.	Class(es)	Date granted
United Kingdom	ns&i & Conker logo *(Figurative)*	2252265	16, 35, 36	16 May 2003
United Kingdom	ns&i logo *(Figurative – series of 4)*	2450780	9, 18, 25, 41	21 Dec 2007
United Kingdom	NS&I logo *(Figurative – series of 4)*	2450757	9, 16, 18, 25, 35, 36, 41	11 Jan 2008
United Kingdom	NS&I Direct Saver	2526485	9, 16, 18, 25, 35, 36, 41	29 Jan 2010
United Kingdom	NSANDI	2450613	9, 16, 35, 36, 41	21 Sept 2007
United Kingdom	nsandi	2450614	9, 16, 35, 36, 41	21 Sept 2007
United Kingdom	NSANDI logo *(Figurative – series of 4)*	2450754	9, 16, 35, 36, 41	21 Sept 2007
United Kingdom	nsandi logo *(Figurative – series of 4)*	2450755	9, 16, 35, 36, 41	21 Sept 2007
United Kingdom	PREMIUM BONDS	2460269	9, 16, 18, 25, 35, 36, 41	25 Jul 2008
United Kingdom	WHERE SAVING BEGINS	3437072	9, 16, 18, 25, 35, 36, 41	10 Jan 2020
United Kingdom	A SPRINGBOARD FOR SAVINGS	3437075	9, 16, 18, 25, 35, 36, 41	10 Jan 2020
United Kingdom	THE SPRINGBOARD EFFECT	3437077	9, 16, 18, 25,35, 36, 41	10 Jan 2020
United Kingdom	NS&I logo *(Figurative – series of 6)*	3437434	9, 16, 18, 25, 35, 36, 41	10 Jan 2020

SCHEDULE 6.1 - IMPLEMENTATION PLAN

1 INTRODUCTION

1.1 This Schedule:

1.1.1 defines the process for the preparation and implementation of the Outline Implementation Plan and Detailed Implementation Plan; and

1.1.2 identifies the Milestones (and associated Deliverables) including the Milestones which trigger payment to the Supplier of the applicable Milestone Payments following the issue of the applicable Milestone Achievement Certificate.

2 DEFINITIONS

2.1 In this Schedule, the following definitions shall apply:

Service Take-over means the date by which all of the Services are being delivered by the Supplier and have been taken over from the outgoing supplier by the Supplier, acknowledging that some Services may have switched over before that point if ready and in accordance with the Implementation Plan.

Transformation Complete means all target solutions have been configured to meet the Director's Requirements and are operational in the Director's production environment, superseding the applicable functions of the prior solutions. It should allow for a period to demonstrate successful live business operation of all service components in target operation. All prior solutions have been decommissioned.

3 OUTLINE IMPLEMENTATION PLAN

3.1 The Outline Implementation Plan is set out in Annex 1.

3.2 All changes to the Outline Implementation Plan shall be subject to the Change Control Procedure provided that the Supplier shall not attempt to postpone any of the Milestones using the Change Control Procedure or otherwise (except in accordance with Clause 33 (*Director Cause*)).

4 APPROVAL OF THE DETAILED IMPLEMENTATION PLAN

4.1 The Supplier shall submit a draft of the Detailed Implementation Plan to the Director for approval within twenty (20) Working Days of the Effective Date.

4.2 The Supplier shall ensure that the draft Detailed Implementation Plan:

4.2.1 incorporates all of the Milestones and Milestone Dates set out in the Outline Implementation Plan;

4.2.2 takes into account implementation plans of other Relevant Third Party Suppliers and any exit plan agreed with Atos IT Services UK Limited as the outgoing supplier;

4.2.3 includes (as a minimum) the Supplier's proposed timescales in respect of the following for each of the Milestones:

(a) the completion of each design document;

(b) the completion of the build phase;

(c) the completion of any Testing to be undertaken in accordance with Schedule 6.2 (*Testing Procedures*);

(d) training and roll-out activities; and

(e) the agreed acceptance criteria for each Deliverable.

4.2.4 clearly outlines all the steps required to implement the Milestones to be achieved in the next twenty-four (24) months, together with a high level plan for the rest of the programme, in conformity with the Director's Requirements;

4.2.5 clearly outlines the required roles and responsibilities of both Parties, including staffing requirements; and

4.2.6 is produced using a software tool as specified, or agreed by the Director.

4.3 Prior to the submission of the draft Detailed Implementation Plan to the Director in accordance with Paragraph 4.1, the Director shall have the right:

4.3.1 to review any documentation produced by the Supplier in relation to the development of the Detailed Implementation Plan, including:

(a) details of the Supplier's intended approach to the Detailed Implementation Plan and its development;

(b) copies of any drafts of the Detailed Implementation Plan produced by the Supplier; and

(c) any other work in progress in relation to the Detailed Implementation Plan; and

4.3.2 to require the Supplier to include any reasonable changes or provisions in the Detailed Implementation Plan.

4.4 Following receipt of the draft Detailed Implementation Plan from the Supplier, the Director shall:

4.4.1 review and comment on the draft Detailed Implementation Plan as soon as reasonably practicable; and

4.4.2 notify the Supplier in writing that it approves or rejects the draft Detailed Implementation Plan no later than twenty (20) Working Days after the date on which the draft Detailed Implementation Plan is first delivered to the Director.

4.5 If the Director rejects the draft Detailed Implementation Plan:

4.5.1 the Director shall inform the Supplier in writing of its reasons for its rejection; and

4.5.2 the Supplier shall then revise the draft Detailed Implementation Plan (taking reasonable account of the Director's comments) and shall re-submit a revised draft Detailed Implementation Plan to the Director for the Director's approval within twenty (20) Working Days of the date of the Director's notice of rejection. The provisions of Paragraph 4.4 and this Paragraph 4.5 shall apply again to any resubmitted draft Detailed Implementation Plan, provided that either Party may refer any disputed matters for resolution by the Dispute Resolution Procedure at any time.

4.6 If the Director approves the draft Detailed Implementation Plan, it shall replace the Outline Implementation Plan from the date of the Director's notice of approval.

5 UPDATES TO AND MAINTENANCE OF THE DETAILED IMPLEMENTATION PLAN

5.1 Following the approval of the Detailed Implementation Plan by the Director:

5.1.1 the Supplier shall submit a revised Detailed Implementation Plan to the Director every three (3) months, starting three (3) months from the Effective Date;

5.1.2 without prejudice to Paragraph 5.1.1, the Director shall be entitled to request a revised Detailed Implementation Plan at any time by giving written notice to the Supplier and the Supplier shall submit a draft revised Detailed Implementation Plan to the Director within twenty (20) Working Days of receiving such a request from the Director (or such longer period as the Parties may agree provided that any failure to agree such longer period shall be referred to the Dispute Resolution Procedure);

5.1.3 any revised Detailed Implementation Plan shall (subject to Paragraph 5.2) be submitted by the Supplier for approval in accordance with the procedure set out in Paragraph 4; and

5.1.4 the Supplier's performance against the Implementation Plan shall be monitored at meetings of the Transformation Committee (as defined in Schedule 8.1 (*Governance*)). In preparation for such meetings, the current Detailed Implementation Plan shall be provided by the Supplier to the Director not less than five (5) Working Days in advance of each meeting of the Transformation Committee.

5.2 Save for any amendments which are of a type identified and notified by the Director (at the Director's discretion) to the Supplier in writing as not requiring approval, any material amendments to the Detailed Implementation Plan shall be subject to the Change Control Procedure provided that:

5.2.1 any amendments to elements of the Detailed Implementation Plan which are based on the contents of the Outline Implementation Plan shall be deemed to be material amendments; and

5.2.2 in no circumstances shall the Supplier be entitled to alter or request an alteration to any Milestone Date except in accordance with Clause 33 (*Director Cause*).

5.3 Any proposed amendments to the Detailed Implementation Plan shall not come into force until they have been approved in writing by the Director.

5.4 Notwithstanding the content of:

5.4.1 the Outline Implementation Plan; or

5.4.2 the Detailed Implementation Plan when approved in accordance with Paragraph 4 and as updated from time to time in accordance with Paragraph 5,

Implementation Services Commencement Date: the later of the date of this Agreement and 23rd October 2023;

Service Take-over commencement: not to occur prior to 1st April 2024;

Service Take-over completion: not later than 31st March 2025;

Transformation Complete: 30th September 2025;

Long Stop Date for all Transformation Complete activities: 31st December 2025.

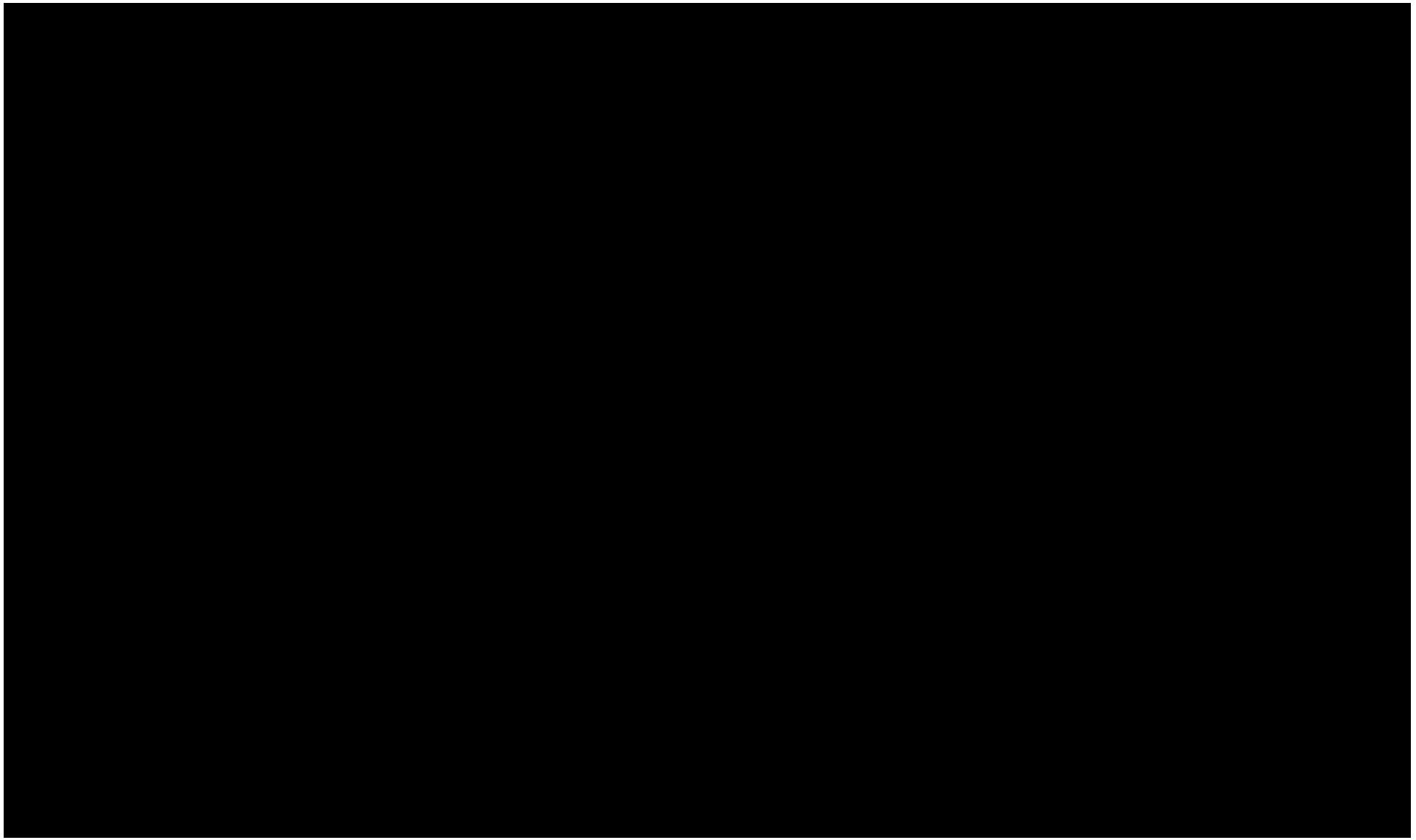
6 ON-BOARDING FUTURE SUPPLIERS AND ADDITIONAL SERVICES

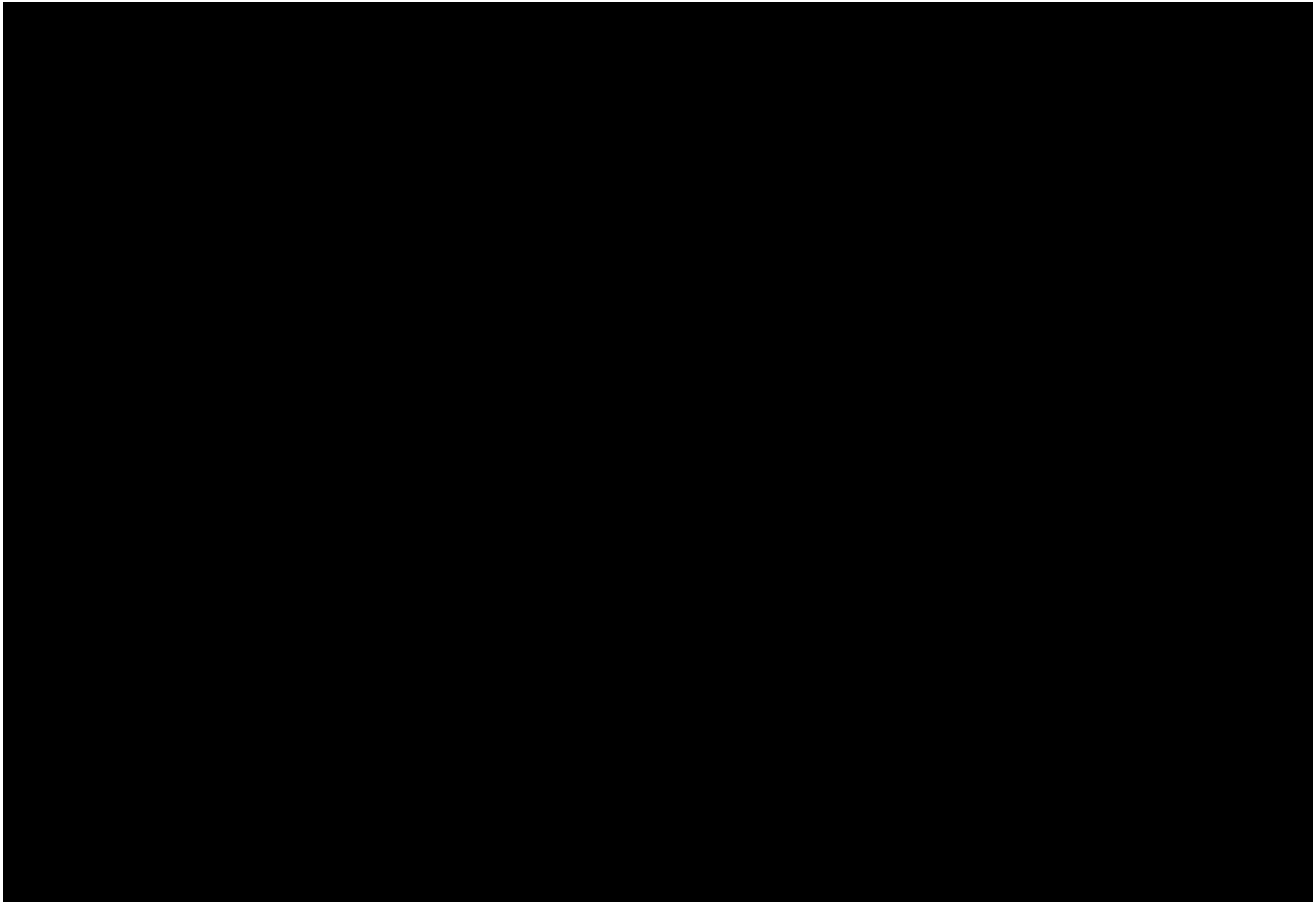
6.1 The process for aligning future on-boarding of Relevant Third Party Suppliers or adding Additional Services and for the preparation and implementation of subsequent Outline Implementation Plans and Detailed Implementation Plans (the "**Additional Services Implementation Plan**") for the on-boarding of those Relevant Third Party Suppliers shall be called off as an Additional Service in accordance with Clause 5.11 (*Additional Services*) and the Multi-Supplier Change Process as set out in Paragraph 16 of Schedule 8.2 (*Change Control Procedure*).

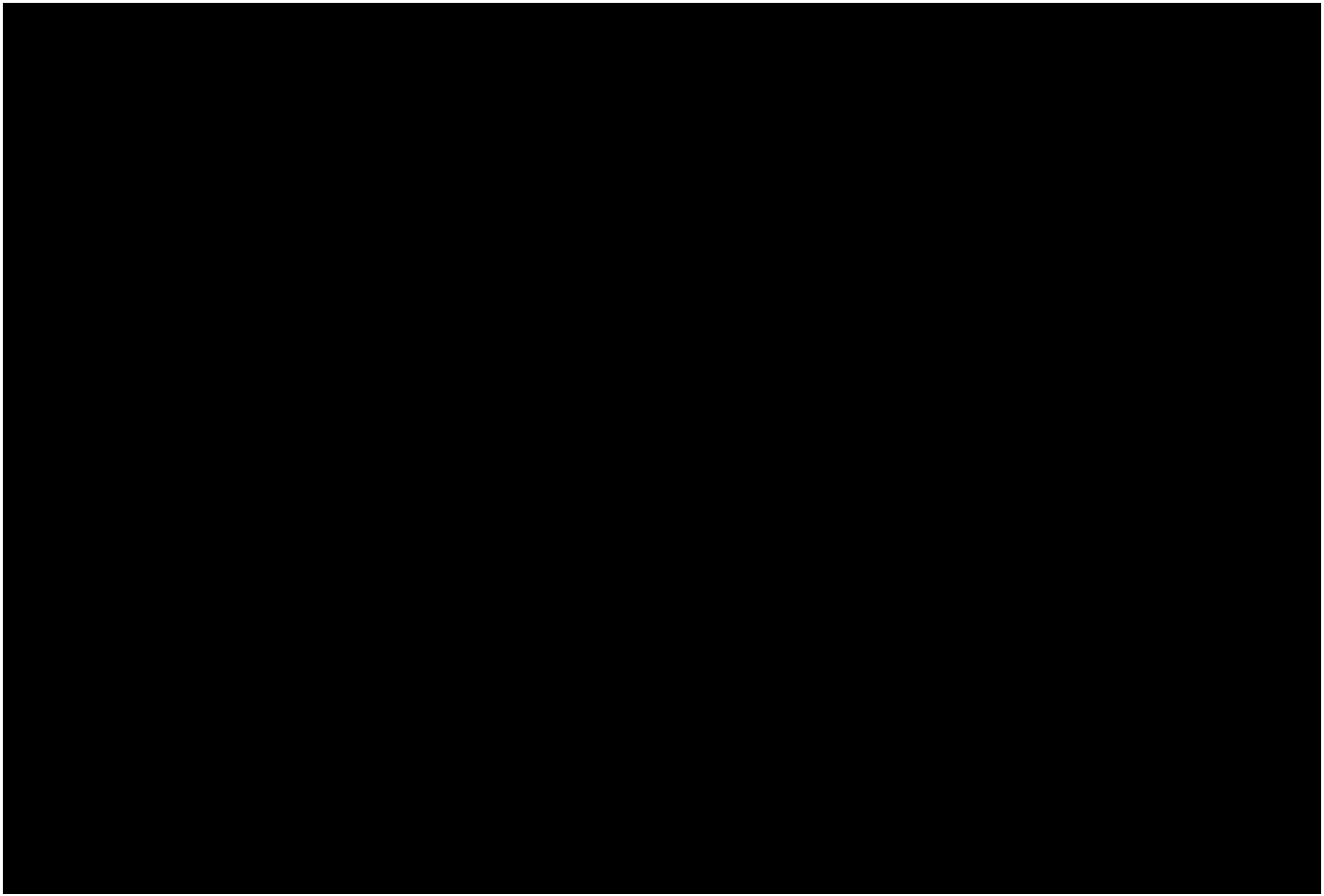
7 GOVERNMENT REVIEWS

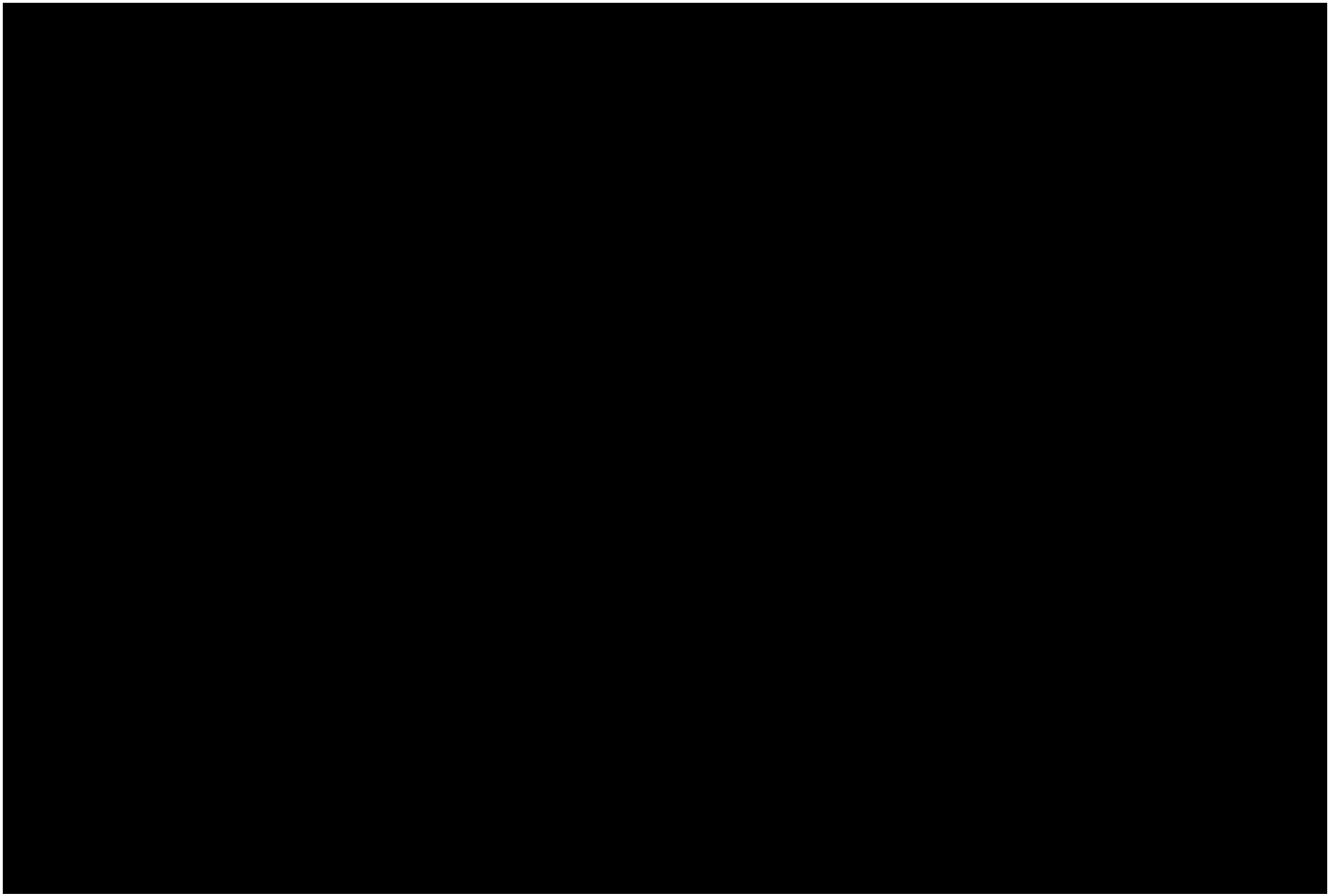
7.1 The Supplier acknowledges that the Services may be subject to review by a Central Government Body at key stages of the project. The Supplier shall cooperate with any bodies undertaking such review and shall allow for such reasonable assistance as may be required for this purpose within the Charges.

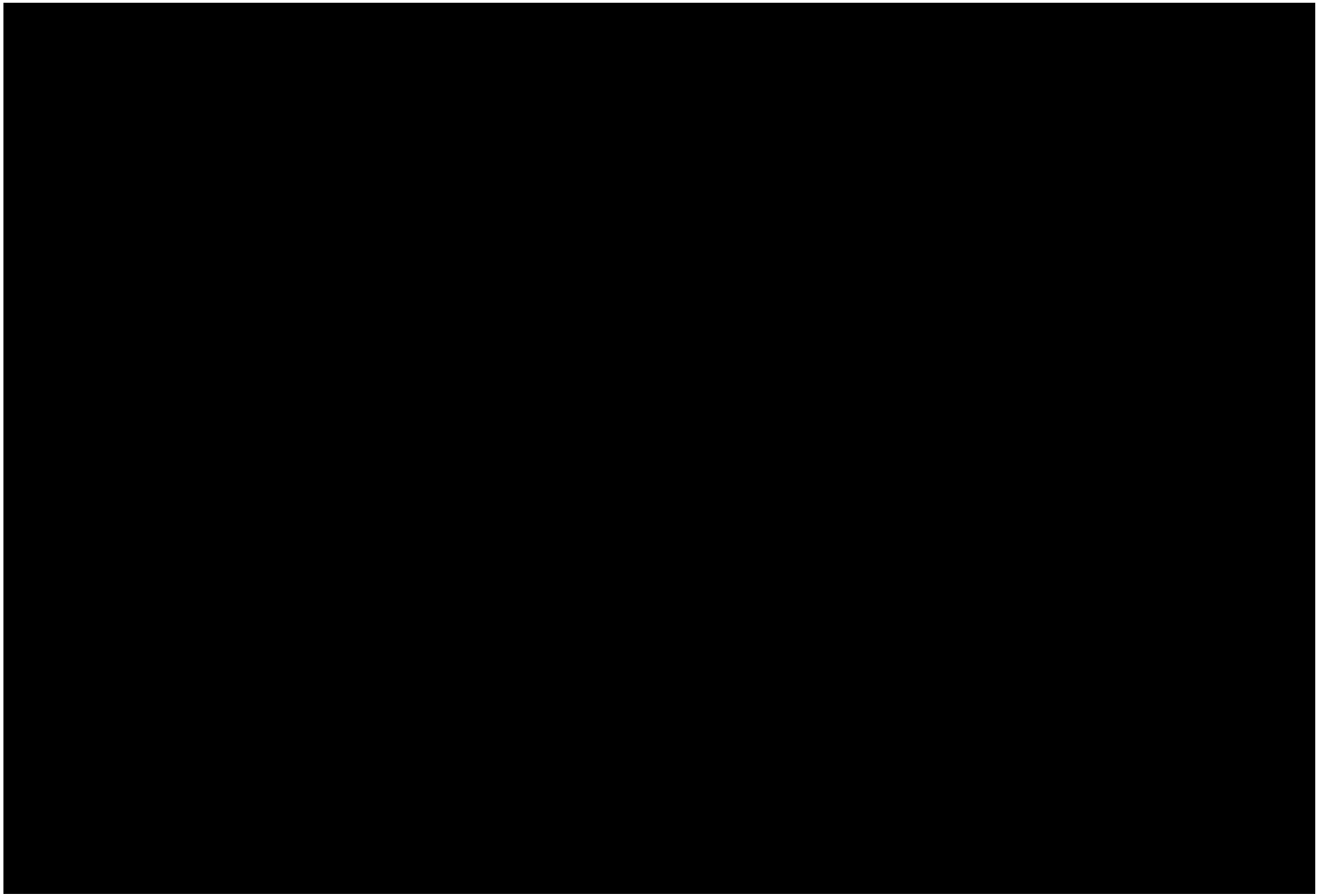
ANNEX 1: OUTLINE IMPLEMENTATION PLAN

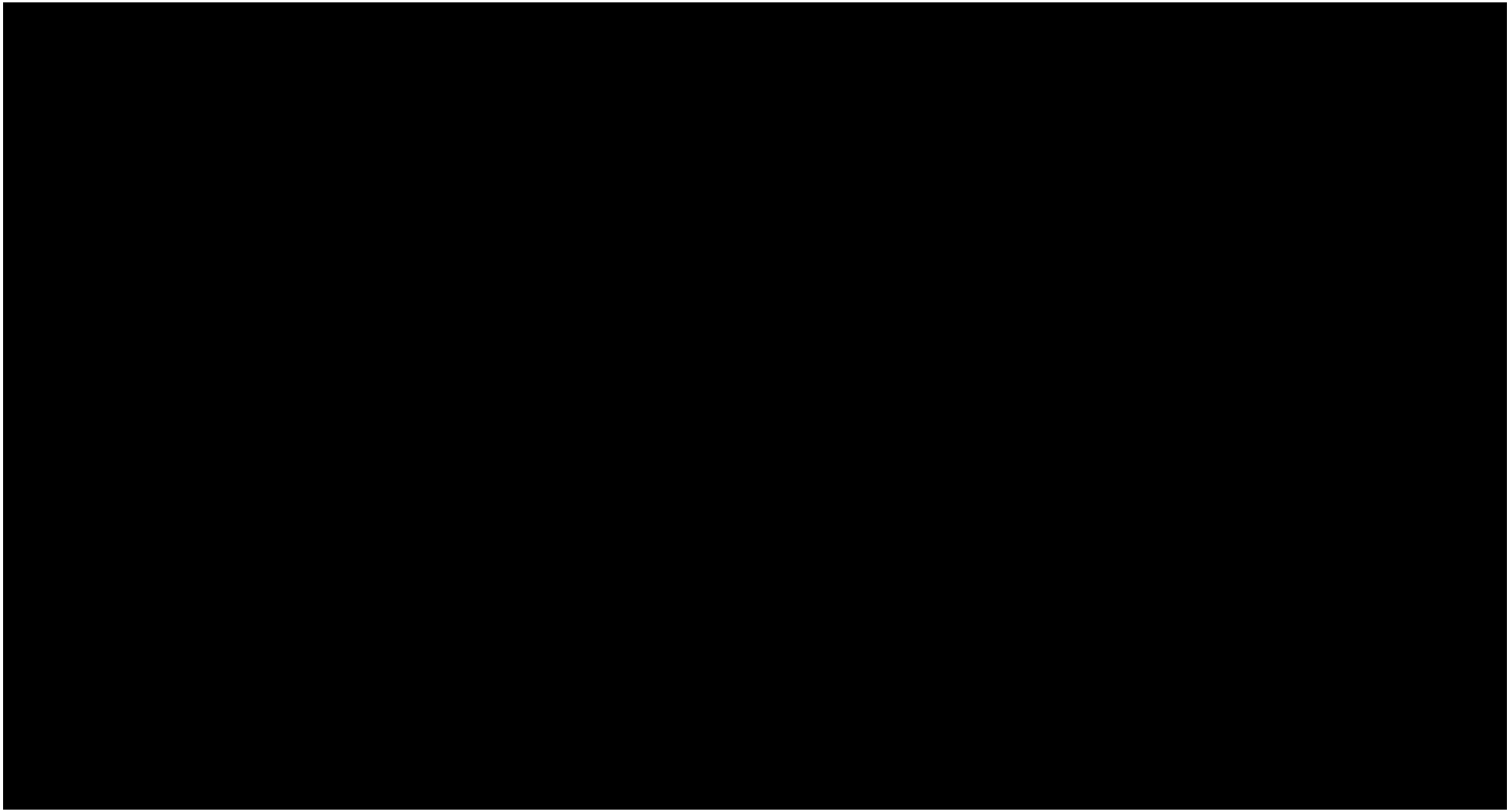












SCHEDULE 6.2 - TESTING PROCEDURES

1 INTRODUCTION AND DEFINITIONS

1.1 This Schedule sets out the process for managing all types of Changes to the Services and the Agreement including the process of implementing projects, initial implementation, on-boarding Relevant Third Party Suppliers and End to End Testing.

1.2 In this Schedule, the following definitions shall apply:

Component means any constituent parts of the infrastructure for a Service, hardware or Software.

End to End Test means the coordinated testing of a beginning to end flow of business processes across multiple services provided by multiple suppliers, as opposed to testing only individual steps or only the Supplier's Services or an element of the Supplier's Services.

Material Test Issue means a Test Issue of Severity Level 1 or Severity Level 2.

Severity Level means the level of severity of a Test Issue, the criteria for which are described in Annex 1 (*Test Issues – Security Levels*).

Test Certificate means a certificate materially in the form of the document contained in Annex 2 issued by the Director when a Deliverable has satisfied its relevant Test Success Criteria.

Test Issue means any variance or non-conformity of a Deliverable from its requirements (such requirements being set out in the relevant Test Success Criteria).

Test Issues Threshold in relation to the Tests applicable to a Milestone, a maximum number of Severity Level 3, Severity Level 4 and Severity Level 5 Test Issues as set out in the relevant Test Plan.

Test Issue Management Log means a log for the recording of Test Issues as described further in Paragraph 9.1.

Test Plan means a plan:

(a) for the Testing of Deliverables; and

(b) setting out other agreed criteria related to the achievement of Milestones,

as described further in Paragraph 5.

Test Reports means the reports to be produced by the Supplier setting out the results of Tests.

Test Specification means the specification that sets out how Tests will demonstrate that the Test Success Criteria have been satisfied, as described in more detail in Paragraph 7.

Test Strategy means a strategy for the conduct of Testing as described further in Paragraph 4.

Test Success Criteria in relation to a Test, the test success criteria for that Test as referred to in Paragraph 6.

Test Witness means any person appointed by the Director pursuant to Paragraph 10.1.

Testing Procedures means the applicable testing procedures and Test Success Criteria set out in this Schedule.

2 RISK

2.1 The issue of a Test Certificate, a Milestone Achievement Certificate and/or a conditional Milestone Achievement Certificate shall not:

2.1.1 operate to transfer any risk that the relevant Deliverable or Milestone is complete or will meet and/or satisfy the Director Requirements for that Deliverable or Milestone; or

2.1.2 affect the Director's right subsequently to reject:

(a) all or any element of the Deliverables to which a Test Certificate relates; or

(b) any Milestone to which the Milestone Achievement Certificate relates.

2.2 Notwithstanding the issuing of any Milestone Achievement Certificate (including the Milestone Achievement Certificate in respect of Authority to Proceed), the Supplier shall remain solely responsible for ensuring that:

2.2.1 the Supplier Solution as designed and developed is suitable for the delivery of the Services and meets the Director Requirements;

2.2.2 the Services are transitioned, implemented and provided in accordance with this Agreement;

2.2.3 there is no negative impact in relation to the delivery of the Services or the services provided by a Relevant Third Party Supplier; and

2.2.4 each Target Performance Level is met from the relevant Operational Service Commencement Date.

3 TESTING OVERVIEW

3.1 The Supplier's methodology for testing, including in relation to Change and implementation, should reflect market approaches to customer focused and test-driven development and the approach to Change in accordance with Paragraph 4 of Schedule 8.2 (*Change Control Procedure*). Notwithstanding any methodology adopted by the Supplier or any processes agreed and incorporated into the Operations Manual (in accordance with Schedule 12 (*Collaboration Agreement*)), the Suppliers approach should reflect the provisions of this Schedule 6.2 (*Testing*), including, but not limited to the provisions of Paragraph 2 (*Risk*).

3.2 All Tests conducted by the Supplier shall be conducted in accordance with the Test Strategy, the Test Plans and the Test Specifications.

3.3 The Supplier shall not submit any Deliverable for Testing:

3.3.1 unless the Supplier is reasonably confident that it will satisfy the relevant Test Success Criteria;

3.3.2 until the Director has issued a Test Certificate in respect of any prior, dependant Deliverable(s); and

3.3.3 until the Parties have agreed the Test Plan and the Test Specification relating to the relevant Deliverable(s).

3.4 The Supplier shall use reasonable endeavours to submit each Deliverable for Testing or re-Testing by or before the date set out in the Implementation Plan for the commencement of Testing in respect of the relevant Deliverable.

3.5 Prior to the issue of a Test Certificate, the Director shall be entitled to review the relevant Test Reports and the Test Issue Management Log. The Test Reports and the Test Issue Management Log shall be submitted to the relevant governance body (as determined by reference to Schedule 8.1

(*Governance*)), together with any other Testing information reasonably required or requested by the Director, at least ten (10) Working Days prior to the date of the relevant governance body meeting.

3.6 Any Disputes between the Director and the Supplier regarding Testing shall be referred to the Dispute Resolution Procedure using the Expedited Dispute Timetable.

4 TEST STRATEGY

4.1 Save where otherwise specified by the Director pursuant to Paragraph 14 (*End to End Tests*), the Supplier shall develop the final Test Strategy as soon as practicable after the Effective Date but in any case no later than thirty (30) Working Days (or such other period as the Parties may agree in writing) after the Effective Date.

4.2 The final Test Strategy shall include:

4.2.1 an overview of how Testing will be conducted in accordance with the Implementation Plan;

4.2.2 the process to be used to capture and record Test results and the categorisation of Test Issues;

4.2.3 the method for mapping the expected Test results to the Test Success Criteria;

4.2.4 the procedure to be followed if a Deliverable fails to satisfy the Test Success Criteria or produces unexpected results, including a procedure for the resolution of Test Issues;

4.2.5 the procedure to be followed to sign off each Test and enable submission of relevant documentation to the relevant governance body;

4.2.6 the process for the production and maintenance of Test Reports and reporting, including templates for the Test Reports and the Test Issue Management Log, and a sample plan for the resolution of Test Issues;

4.2.7 the names and contact details of the Director's and the Supplier's Test representatives;

4.2.8 a high level identification of the resources required for Testing, including facilities, infrastructure, personnel and Director and/or third party involvement (including, where applicable, Customers) in the conduct of the Tests;

4.2.9 the technical environments required to support the Tests; and

4.2.10 the procedure for managing the configuration of the Test environments.

5 TEST PLANS

5.1 Save where otherwise specified by the Director pursuant to Paragraph 14 (*End to End Tests*), the Supplier shall develop Test Plans and submit these for the approval of the Director as soon as practicable but in any case no later than twenty (20) Working Days (or such other period as the Parties may agree in the Test Strategy or otherwise agree in writing) prior to the start date for the relevant Testing (as specified in the Implementation Plan).

5.2 Each Test Plan shall include as a minimum:

5.2.1 the relevant Test definition and the purpose of the Test, the Milestone to which it relates, the requirements being tested and, for each Test, the specific Test Success Criteria to be satisfied;

5.2.2 a detailed procedure for the Tests to be carried out, including:

(a) the timetable for the Tests, including start and end dates;

(b) the Testing mechanism;

(c) dates and methods by which the Director can inspect Test results or witness the Tests in order to establish that the Test Success Criteria have been met;

(d) the mechanism for ensuring the quality, completeness and relevance of the Tests;

(e) the format and an example of Test progress reports and the process with which the Director accesses daily Test schedules;

(f) the process which the Director will use to review Test Issues and the Supplier's progress in resolving these in a timely basis;

(g) the Test schedule;

(h) the re-Test procedure, the timetable and the resources which would be required for re-Testing; and

5.2.3 the process for escalating Test Issues from a re-Test situation to the taking of specific remedial action to resolve the Test Issue.

5.3 The Director shall not unreasonably withhold or delay its approval of the Test Plans provided that the Supplier shall incorporate any reasonable requirements of the Director in the Test Plans.

6 TEST SUCCESS CRITERIA

6.1 Save where set out in Annex 4, the Test Success Criteria for each Test that must be Achieved for the Supplier to Achieve either the ATP Milestone or a CPP Milestone and all other Tests shall be agreed between the Parties as part of the relevant Test Plan pursuant to Paragraph 5 and/or Paragraph 14 (as applicable).

7 TEST SPECIFICATION

7.1 Following approval of a Test Plan, unless otherwise specified by the Director pursuant to Paragraph 14, the Supplier shall develop the Test Specification for the relevant Deliverables as soon as reasonably practicable and in any event at least ten (10) Working Days (or such other period as the Parties may agree in the Test Strategy or otherwise agree in writing) prior to the start of the relevant Testing (as specified in the Implementation Plan).

7.2 Each Test Specification shall include as a minimum:

7.2.1 the specification of the Test data, including its source, scope, volume and management, a request (if applicable) for relevant Test data to be provided by the Director and the extent to which it is equivalent to live operational data;

7.2.2 a plan to make the resources available for Testing;

7.2.3 Test scripts;

7.2.4 Test pre-requisites and the mechanism for measuring them; and

7.2.5 expected Test results, including:

(a) a mechanism to be used to capture and record Test results; and

(b) a method to process the Test results to establish their content.

8 TESTING

8.1 Before submitting any Deliverables for Testing the Supplier shall subject the relevant Deliverables to its own internal quality control measures.

8.2 The Supplier shall manage the progress of Testing in accordance with the relevant Test Plan and shall carry out the Tests in accordance with the relevant Test Specification. Tests may be witnessed by the Test Witnesses in accordance with Paragraph 10.

8.3 The Supplier shall notify the Director at least ten (10) Working Days (or such other period as the Parties may agree in writing) in advance of the date, time and location of the relevant Tests and the Director shall ensure that the Test Witnesses attend the Tests, except where the Director has specified in writing that such attendance is not necessary.

8.4 The Director may raise and close Test Issues during the Test witnessing process.

8.5 The Supplier shall provide to the Director in relation to each Test:

8.5.1 a draft Test Report not less than two (2) Working Days (or such other period as the Parties may agree in writing) prior to the date on which the Test is planned to end; and

8.5.2 the final Test Report within five (5) Working Days (or such other period as the Parties may agree in writing) of completion of Testing.

8.6 Each Test Report shall provide a full report on the Testing conducted in respect of the relevant Deliverables, including:

8.6.1 an overview of the Testing conducted;

8.6.2 identification of the relevant Test Success Criteria that have been satisfied;

8.6.3 identification of the relevant Test Success Criteria that have not been satisfied together with the Supplier's explanation of why those criteria have not been met;

8.6.4 the Tests that were not completed together with the Supplier's explanation of why those Tests were not completed;

8.6.5 the Test Success Criteria that were satisfied, not satisfied or which were not tested, and any other relevant categories, in each case grouped by Severity Level in accordance with Paragraph 9.1; and

8.6.6 the specification for any hardware and software used throughout Testing and any changes that were applied to that hardware and/or software during Testing.

9 TEST ISSUES

9.1 Where a Test Report identifies a Test Issue, the Parties shall agree the classification of the Test Issue using the criteria specified in Annex 1 and the Test Issue Management Log maintained by the Supplier shall log Test Issues reflecting the Severity Level allocated to each Test Issue.

9.2 The Supplier shall be responsible for maintaining the Test Issue Management Log and for ensuring that its contents accurately represent the current status of each Test Issue at all relevant times. The Supplier shall make the Test Issue Management Log available to the Director upon request.

9.3 The Director shall confirm the classification of any Test Issue unresolved at the end of a Test in consultation with the Supplier. If the Parties are unable to agree the classification of any unresolved Test Issue, the Dispute shall be dealt with in accordance with the Dispute Resolution Procedure using the Expedited Dispute Timetable.

10 TEST WITNESSING

10.1 The Director may, in its sole discretion, require the attendance at any Test of one or more Test Witnesses selected by the Director, each of whom shall have appropriate skills to fulfil the role of a Test Witness.

10.2 The Supplier shall give the Test Witnesses access to any documentation and Testing environments reasonably necessary and requested by the Test Witnesses to perform their role as a Test Witness in respect of the relevant Tests.

10.3 The Test Witnesses:

10.3.1 shall actively review the Test documentation;

10.3.2 will attend and engage in the performance of the Tests on behalf of the Director so as to enable the Director to gain an informed view of whether a Test Issue may be closed or whether the relevant element of the Test should be re-Tested;

10.3.3 shall not be involved in the execution of any Test;

10.3.4 shall be required to verify that the Supplier conducted the Tests in accordance with the Test Success Criteria and the relevant Test Plan and Test Specification;

10.3.5 may produce and deliver their own, independent reports on Testing, which may be used by the Director to assess whether the Tests have been Achieved;

10.3.6 may raise Test Issues on the Test Issue Management Log in respect of any Testing; and

10.3.7 may require the Supplier to demonstrate the modifications made to any defective Deliverable before a Test Issue is closed.

11 TEST QUALITY AUDIT

11.1 Without prejudice to its rights pursuant to Clause 12.2.2 (*Records, Reports, Audits & Open Book Data*), the Director may perform on-going quality audits in respect of any part of the Testing (each a "**Testing Quality Audit**") subject to the provisions set out in the agreed Quality Plan.

11.2 The focus of the Testing Quality Audits shall be on:

11.2.1 adherence to an agreed methodology;

11.2.2 adherence to the agreed Testing process;

11.2.3 adherence to the Quality Plan;

11.2.4 review of status and key development issues; and

11.2.5 identification of key risk areas.

11.3 The Supplier shall allow sufficient time in the Test Plan to ensure that adequate responses to a Testing Quality Audit can be provided.

11.4 The Director will give the Supplier at least five (5) Working Days' written notice of the Director's intention to undertake a Testing Quality Audit and the Supplier may request, following receipt of that notice, that any Testing Quality Audit be delayed by a reasonable time period if in the Supplier's reasonable opinion, the carrying out of a Testing Quality Audit at the time specified by the Director will materially and adversely impact the Implementation Plan.

11.5 A Testing Quality Audit may involve document reviews, interviews with the Supplier Personnel involved in or monitoring the activities being undertaken pursuant to this Schedule, the Director witnessing Tests and demonstrations of the Deliverables to the Director. Any Testing Quality Audit shall be limited

in duration to a maximum time to be agreed between the Supplier and the Director on a case by case basis (such agreement not to be unreasonably withheld or delayed). The Supplier shall provide all reasonable necessary assistance and access to all relevant documentation required by the Director to enable it to carry out the Testing Quality Audit.

11.6 If the Testing Quality Audit gives the Director concern in respect of the Testing Procedures or any Test, the Director shall:

11.6.1 discuss the outcome of the Testing Quality Audit with the Supplier, giving the Supplier the opportunity to provide feedback in relation to specific activities; and

11.6.2 subsequently prepare a written report for the Supplier detailing its concerns,

and the Supplier shall, within a reasonable timeframe, respond in writing to the Director's report.

11.7 In the event of an inadequate response to the Director's report from the Supplier, the Director (acting reasonably) may withhold a Test Certificate (and consequently delay the grant of a Milestone Achievement Certificate) until the issues in the report have been addressed to the reasonable satisfaction of the Director.

12 OUTCOME OF TESTING

12.1 The Director shall issue a Test Certificate as soon as reasonably practicable when the Deliverables satisfy the Test Success Criteria in respect of that Test without any Test Issues.

12.2 If the Deliverables (or any relevant part) do not satisfy the Test Success Criteria then the Director shall notify the Supplier and:

12.2.1 the Director may issue a Test Certificate conditional upon the remediation of the Test Issues;

12.2.2 where the Parties agree that there is sufficient time prior to the relevant Milestone Date, the Director may extend the Test Plan by such reasonable period or periods as the Parties may reasonably agree and require the Supplier to rectify the cause of the Test Issue and re-submit the Deliverables (or the relevant part) to Testing; or

12.2.3 where the failure to satisfy the Test Success Criteria results, or is likely to result, in the failure (in whole or in part) by the Supplier to meet a Milestone, then without prejudice to the Director's other rights and remedies, such failure shall constitute a Notifiable Default for the purposes of Clause 29.1 (*Rectification Plan Process*).

12.3 The Director shall be entitled, without prejudice to any other rights and remedies that it has under this Agreement, to recover from the Supplier any reasonable additional costs it may incur as a direct result of further review or re-Testing which is required for the Test Success Criteria for that Deliverable to be satisfied.

13 ISSUE OF MILESTONE ACHIEVEMENT CERTIFICATE

13.1 The Director shall issue a Milestone Achievement Certificate in respect of a given Milestone as soon as is reasonably practicable following:

13.1.1 the issuing by the Director of Test Certificates and/or conditional Test Certificates in respect of all Deliverables related to that Milestone which are due to be Tested; and

13.1.2 performance by the Supplier to the reasonable satisfaction of the Director of any other tasks identified in the Implementation Plan as associated with that Milestone (which may include the submission of a Deliverable that is not due to be Tested, such as the production of Documentation).

13.2 The grant of a Milestone Achievement Certificate shall entitle the Supplier to the receipt of a payment in respect of that Milestone in accordance with the provisions of Schedule 7.1 (*Charges and Invoicing*).

13.3 If a Milestone is not Achieved, the Director shall promptly issue a report to the Supplier setting out:

13.3.1 the applicable Test Issues; and

13.3.2 any other reasons for the relevant Milestone not being Achieved.

13.4 If there are Test Issues but these do not exceed the Test Issues Threshold, then provided there are no Material Test Issues, the Director shall issue a Milestone Achievement Certificate.

13.5 Without prejudice to the Director's other remedies the following shall constitute a Notifiable Default for the purposes of Clause 29.1 (*Rectification Plan Process*) and the Director shall refuse to issue a Milestone Achievement Certificate where:

13.5.1 there is one or more Material Test Issue(s); or

13.5.2 the information required under Schedule 8.4 (*Reports and Records Provisions*) Annex 3 (*Records to upload to Virtual Library*) has not been uploaded to the Virtual Library in accordance with Paragraph 4 of that Schedule.

13.6 If there are Test Issues which exceed the Test Issues Threshold but there are no Material Test Issues, the Director may at its discretion (without waiving any rights in relation to the other options) choose to issue a Milestone Achievement Certificate conditional on the remediation of the Test Issues in accordance with an agreed Rectification Plan provided that:

13.6.1 any Rectification Plan shall be agreed before the issue of a conditional Milestone Achievement Certificate unless the Director agrees otherwise (in which case the Supplier shall submit a Rectification Plan for approval by the Director within ten (10) Working Days of receipt of the Director's report pursuant to Paragraph 13.3); and

13.6.2 where the Director issues a conditional Milestone Achievement Certificate, it may (but shall not be obliged to) revise the failed Milestone Date and any subsequent Milestone Date.

14 END TO END TESTS

14.1 The Director reserves the right to nominate a lead (the "**Lead Supplier**"), as notified from time to time by the Director, to act on its behalf to undertake any or all of the Director's activities and responsibilities in respect of End to End Testing as set out in this Paragraph 14. The Lead Supplier shall co-ordinate activity across the delivery of End to End Testing as instructed by the Director.

14.2 The Supplier shall, at the request of the Director or the Lead Supplier and pursuant to its obligations under the Collaboration Agreement, cooperate with the Director, the Lead Supplier and any Relevant Third Party Supplier and participate in End to End Testing including (but not limited to):

14.2.1 in relation to the on-boarding of a Relevant Third Party Supplier;

14.2.2 whenever a significant implementation is progressing through delivery,

14.2.3 a Change; or

14.2.4 in other such circumstances as the Director may at its discretion request.

14.3 In the event of an End to End Test, the Director shall develop the Test Strategy, Test Plan and Test Specification and provide a copy of the same to the Supplier for the purpose of the Supplier carrying out the Tests on any Deliverable for which it is responsible or any element of its Services that form part of or impact on the End to End Test.

14.4 The Supplier shall provide all reasonable cooperation, assistance and information in relation to the development of the Test Strategy, Test Plan and Test Specification for the End to End Test as requested by the Director.

14.5 The relevant Test Success Criteria shall be determined as part of the relevant Test Plan.

14.6 The provisions of Paragraphs 8 to 13 of this Schedule 6.2 (*Testing Procedures*) shall apply in relation to the Supplier's testing of its own Services or Deliverables as part of the End to End Test.

14.7 For the avoidance of doubt the Supplier shall be responsible for the resolution of any Test Issues arising in relation to the End to End Test and shall cooperate with the Director and Relevant Third Party Supplier in the resolution of any wider Test Issues.

ANNEX 1: TEST ISSUES – SEVERITY LEVELS

1 **Severity Level 1 Test Issue**: a Test Issue that causes non-recoverable conditions, e.g. it is not possible to continue using a Component, a Component crashes, there is database or file corruption, or data loss;

2 **Severity Level 2 Test Issue**: a Test Issue for which, as reasonably determined by the Director, there is no practicable workaround available, and which:

2.1 causes a Component to become unusable;

2.2 causes a lack of functionality, or unexpected functionality, that has an impact on the current Test; or

2.3 has an adverse impact on any other Component(s) or any other area of the Services;

3 **Severity Level 3 Test Issue:** a Test Issue which:

3.1 causes a Component to become unusable;

3.2 causes a lack of functionality, or unexpected functionality, but which does not impact on the current Test; or

3.3 has an impact on any other Component(s) or any other area of the Services;

but for which, as reasonably determined by the Director, there is a practicable workaround available;

4 **Severity Level 4 Test Issue**: a Test Issue which causes incorrect functionality of a Component or process, but for which there is a simple, Component based, workaround, and which has no impact on the current Test, or other areas of the Services; and

5 **Severity Level 5 Test Issue:** a Test Issue that causes a minor problem, for which no workaround is required, and which has no impact on the current Test, or other areas of the Services.

ANNEX 2: TEST CERTIFICATE

To: **[*NAME OF SUPPLIER*]**

FROM: **[*NAME OF DIRECTOR*]**

[*Date*]

Dear Sirs,

TEST CERTIFICATE

Deliverables: **[*insert description of Deliverables*]**

We refer to the agreement (the "**Agreement**") relating to the provision of the Services between the [***name of Director***] (the "**Director**") and [***name of Supplier***] (the "**Supplier**") dated [***date***].

Capitalised terms used in this certificate have the meanings given to them in Schedule 1 (*Definitions*) or Schedule 6.2 (*Testing Procedures*) of the Agreement.

[We confirm that the Deliverables listed above have been tested successfully in accordance with the Test Plan relevant to those Deliverables.]

OR

[This Test Certificate is issued pursuant to Paragraph 12.1 of Schedule 6.2 (*Testing Procedures*) of the Agreement on the condition that any Test Issues are remedied in accordance with the Rectification Plan attached to this certificate.]*

**delete as appropriate*

Yours faithfully

[***Name***]

[***Position***]

acting on behalf of [***name of Director***]

ANNEX 3: MILESTONE ACHIEVEMENT CERTIFICATE

To: [***NAME OF SUPPLIER***]

FROM: [***NAME OF DIRECTOR***]

[***Date***]

Dear Sirs,

MILESTONE ACHIEVEMENT CERTIFICATE

Milestone: [***insert description of Milestone***]

We refer to the agreement (the "**Agreement**") relating to the provision of the Services between the [***name of Director***] (the "**Director**") and [***name of Supplier***] (the "**Supplier**") dated [***date***].

Capitalised terms used in this certificate have the meanings given to them in Schedule 1 (*Definitions*) or Schedule 6.2 (*Testing Procedures*) of the Agreement.

[We confirm that all the Deliverables relating to Milestone [***number***] have been tested successfully in accordance with the Test Plan relevant to this Milestone [or that a conditional Test Certificate has been issued in respect of those Deliverables that have not satisfied the relevant Test Success Criteria.]]*

OR

[This Milestone Achievement Certificate is granted pursuant to Paragraph 13.1 of Schedule 6.2 (*Testing Procedures*) of the Agreement on the condition that any Test Issues are remedied in accordance with the Rectification Plan attached to this certificate.]*

[You may now issue an invoice in respect of the Milestone Payment associated with this Milestone in accordance with the provisions of Schedule 7.1 (*Charges and Invoicing*)]*

*delete as appropriate

Yours faithfully

[***Name***]

[***Position***]

acting on behalf of [***Director***]

ANNEX 4: TEST SUCCESS CRITERIA

1 Tests to be Achieved in order to Achieve an ATP Milestone (see SCHEDULE 6.1 - IMPLEMENTATION PLAN - ANNEX 1: OUTLINE IMPLEMENTATION PLAN)

Test	Pre-conditions*	Test Success Criteria
Solution Readiness	Evidence provided for satisfactory Testing completion reports (Unit, SIT, UAT and OAT), Data Migration reports, a Detailed Production System Cutover Plan Agreed and on-track, security test completion report.	Agreement and Approval at Operational Readiness that evidence provided is satisfactory and any remaining exceptions are being managed appropriately to enable the related OSCD.
Technical Readiness	Evidence provided for satisfactory Performance, Failover and Resilience Testing achievement reports.	Agreement and Approval at Operational Readiness that evidence provided is satisfactory and any remaining exceptions are being managed appropriately to enable the related OSCD.
Business Readiness	Evidence provided for service resourcing confirmed, staff transfer on track, users and business roles mapped, communications plan on track, sites ready, training completion report, SLA and KPI reporting readiness evidenced.	Agreement and Approval at Operational Readiness that evidence provided is satisfactory and any remaining exceptions are being managed appropriately to enable the related OSCD.
Support Readiness	Evidence provided for service desk (including ServiceNow) and the lines of support readiness report, early life support resourced and in place.	Agreement and Approval at Operational Readiness that evidence provided is satisfactory and any remaining exceptions are being managed appropriately to enable the related OSCD.

* Note: The Pre-Conditions are that e.g. the Success Criteria for the previous Tests must be satisfied before the ATP Milestone tests are commenced.

2 Tests to be Achieved in order to Achieve a CPP Milestones (see SCHEDULE 6.1 - IMPLEMENTATION PLAN - ANNEX 1: OUTLINE IMPLEMENTATION PLAN)

CPP Milestone Charge No.	Test	Test Success Criteria
[All]	Evidenced the demonstration of successful live business operation of all service components related to the respective OSCD.	Agreement and Approval to end Early Life Support period after related OSCD based on the evidence provided is satisfactory and any remaining exceptions are being managed

		appropriately in continuous improvement.

All such other Tests and Test Success Criteria required to demonstrate acceptance of a Service and/or Deliverable and issue of the Test Certificate and/or Milestone Achievement Certification shall be agreed between the Parties as part of the relevant Test Plan in accordance with Paragraph 5 of this Schedule 6.2 (*Testing Procedures*).

SCHEDULE 7.1 - CHARGES AND INVOICING

1 DEFINITIONS

1.1 In this Schedule, the following definitions shall apply:

Achieved Profit Margin means the cumulative Supplier Profit Margin calculated from (and including) the Effective Date (or, if applicable, the date of the last adjustment to the Charges made pursuant to Paragraph 2.2 of Part 4) to (and including) the last day of the previous Contract Year.

Agent means the Supplier acting as intermediary for the procurement of certain postal and telephony services (monitored and/or regulated by Ofcom or its equivalent) from its Sub-contractors.

Anticipated Contract Life Profit Margin means the anticipated Supplier Profit Margin over the Term as reflected in the Financial Model.

Baseline Volume means the number of transactions for each component of the Service which is included in the Fixed Service Charge and is set out in Schedule 7.1 (*Charges and Invoicing*) in Appendix 2 to Part 2 – Charging Mechanisms.

Certificate of Costs means a certificate of costs signed by the Supplier's Chief Financial Officer or Director of Finance (or equivalent as agreed in writing by the Director in advance of issue of the relevant certificate) and substantially in the format set out in Annex 2.

Charging Model means the charging model outlining details of the Milestone Payments, Service Charges, Pass Through Items, Additional Services, and Reward Pot to be developed by the Supplier and approved by the Director in accordance with Paragraph 2 of this Schedule 7.1 (*Charges and Invoicing*).

Costs means the following costs (without double recovery) to the extent that they are reasonably and properly incurred by the Supplier in providing the Services:

(a) the cost to the Supplier or the Key Sub-contractor (as the context requires), calculated per Work Day, of engaging the Supplier Personnel, including:

(i) base salary paid to the Supplier Personnel;

(ii) employer's national insurance contributions;

(iii) Employer Pension Contributions;

(iv) car allowances;

(v) any other contractual employment benefits;

(vi) staff training;

(vii) work place accommodation;

(viii) work place IT equipment and tools reasonably necessary to perform the Services (but not including items included within limb (b) below); and

(ix) reasonable recruitment costs, as agreed with the Director;

(b) costs incurred in respect of those Assets which are detailed on the Registers and which would be treated as capital costs according to generally accepted accounting principles within the UK, which shall include the cost to be charged in respect of Assets by the Supplier to the

Director or (to the extent that risk and title in any Asset is not held by the Supplier) any cost actually incurred by the Supplier in respect of those Assets;

(c) operational costs which are not included within (a) or (b) above, to the extent that such costs are necessary and properly incurred by the Supplier in the delivery of the Services;

(d) Forecast Contingency Costs;

(e) Reimbursable Expenses to the extent these are incurred in delivering any Services where the Charges for those Services are to be calculated on a Fixed Price or Firm Price pricing mechanism;

but excluding:

(i) Overhead;

(ii) financing or similar costs;

(iii) maintenance and support costs to the extent that these relate to maintenance and/or support services provided beyond the Term, whether in relation to Assets or otherwise;

(iv) taxation;

(v) fines and penalties;

(vi) amounts payable under Schedule 7.3 (*Benchmarking*); and

(vii) non-cash items (including depreciation, amortisation, impairments and movements in provisions).

Employer Pension Contributions means such employer pension contributions, charges or costs incurred by the Supplier which have been expressly agreed by the Director in writing to constitute 'Employer Pension Contributions'.

Fixed Service Charge means the component of the monthly Service Charge that is fixed in advance as set out in the Charging Model for the month falling in the applicable Service Period (or, if the Charging Model has not yet been approved by the Director in accordance with Paragraph 2 of this Schedule 7.1 (*Charges and Invoicing*), the Pricing Response Template).

Forecast Contingency Costs means the costs which the Supplier forecasts may be incurred in relation to the Allowable Assumptions and contingencies that are identified in the Pricing Response Template, such costs being those set out in the column headed 'Forecast Contingency Costs' in the Pricing Response Template (as such costs are updated from time to time).

Indexation and **Index** means the adjustment of an amount or sum in accordance with Paragraph 6 of Part 3.

Maximum Permitted Profit Margin means the Anticipated Contract Life Profit Margin plus five percent (5%).

Overhead means those amounts which are intended to recover a proportion of the Supplier's or the Key Sub-contractor's (as the context requires) indirect corporate costs (including financing, marketing, advertising, research and development and insurance costs and any fines or penalties) but excluding allowable indirect costs apportioned to facilities and administration in the provision of Supplier Personnel and accordingly included within limb (a) of the definition of "Costs".

Pass Through Items means those items identified in Paragraph 9 of this Schedule and any other items which the Parties agree should be charged for on a pass through basis which shall be charged to the Director at cost without the application of the Supplier Profit Margin or any other charges.

Pass Through Items (Supplier Acting As Agent) means those items identified in Paragraph 10.1 of Part 1 of this Schedule and any other items which the Parties agree in writing should be charged for a pass through (supplier acting as agent) basis and which are provided on the basis that the Supplier is acting as an Agent for the provision of such item(s).

Pricing Response Template means the excel spreadsheet contained in the Excel File reference "*17.1 Annex 1 Schedule 7.1 Pricing Response Template*", as referenced at Annex 1 (*Pricing Response Template*) which sets out the Charges and payment profile for the Charges, as amended in accordance with this Schedule.

Reimbursable Expenses means reasonable out of pocket travel and subsistence (for example, hotel and food) expenses, properly and necessarily incurred in the performance of the Services, calculated at the rates and in accordance with the Director's expenses policy current from time to time, but not including:

(a) travel expenses incurred as a result of Supplier Personnel travelling to and from their usual place of work, or to and from the premises at which the Services are principally to be performed, unless the Director otherwise agrees in advance in writing; and

(b) subsistence expenses incurred by Supplier Personnel whilst performing the Services at their usual place of work, or to and from the premises at which the Services are principally to be performed.

Reward Pot as defined in the Collaboration Agreement.

Service Period means the month in which the Service was provided by the Supplier.

Supplier Profit in relation to a period or a Milestone (as the context requires), the difference between the total Charges (in nominal cash flow terms but excluding any Deductions) and total Costs (in nominal cash flow terms) for the relevant period or in relation to the relevant Milestone.

Supplier Profit Margin in relation to a period or a Milestone (as the context requires), the Supplier Profit for the relevant period or in relation to the relevant Milestone divided by the total Charges over the same period or in relation to the relevant Milestone and expressed as a percentage.

Supporting Documentation means sufficient information in writing to enable the Director reasonably to assess whether the Charges, Reimbursable Expenses and other sums due from the Director detailed in the information are properly payable, including copies of any applicable Milestone Achievement Certificates or receipts.

Universal Standing Charge the amount to be determined by the Director on each anniversary of the Agreement and used to determine the Reward Pot.

Variable Service Charge means the Charge for the number of transactions counted by the Supplier that are higher than the Baseline Volume included in the relevant Fixed Charge in a month.

Verification Period in relation to an Allowable Assumption, the period in which the Forecast Contingency Costs have been apportioned in the "Allocation of Forecast Contingency Costs" part of the Allowable Assumptions table in tabs B2a and B2b of the Pricing Response Template.

Work Day means 7.5 Work Hours, whether or not such hours are worked consecutively and whether or not they are worked on the same day.

Work Hours means the hours spent by the Supplier Personnel properly working on the Services including time spent travelling (other than to and from the Supplier's offices, or to and from the Sites) but excluding lunch breaks.

PART 1: PRICING

1 PRICING RESPONSE TEMPLATE

1.1 The Pricing Response Template is set out in Annex 1.

1.2 All changes to the Pricing Response Template shall be subject to the Change Control Procedure provided that the Supplier shall not attempt to postpone any of the Milestones using the Change Control Procedure or otherwise (except in accordance with Clause 33 (*Director Cause*)).

2 APPROVAL OF THE CHARGING MODEL

2.1 The Supplier shall submit a draft of the Charging Model to the Director for approval within twenty (20) Working Days of the Effective Date.

2.2 The Supplier shall ensure that the draft Charging Model:

2.2.1 incorporates all of the Milestone Payments and Service Charges set out in the Pricing Response Template;

2.2.2 sets out detailed information around incremental costs during delivery of the Implementation Services, including for each Milestone:

(a) details of the costs to be recovered upon Achievement of the relevant Milestone; and

(b) the proposed operational costs that will be charged for each month following such Achievement; and

2.2.3 is produced in a format or using a software tool as specified, or agreed by, the Director.

2.3 Prior to the submission of the draft Charging Model to the Director in accordance with Paragraph 2.1, the Director shall have the right:

2.3.1 to review any documentation produced by the Supplier in relation to the development of the Charging Model, including:

(a) details of the Supplier's intended approach to the Charging Model and its development;

(b) copies of any drafts of the Charging Model produced by the Supplier; and

(c) any other work in progress in relation to the Charging Model; and

2.3.2 to require the Supplier to include any reasonable changes or provisions in the Charging Model.

2.4 Following receipt of the draft Charging Model from the Supplier, the Director shall:

2.4.1 review and comment on the draft Charging Model as soon as reasonably practicable; and

2.4.2 notify the Supplier in writing that it approves or rejects the draft Charging Model no later than twenty (20) Working Days after the date on which the draft Charging Model is first delivered to the Director.

2.5 If the Director rejects the draft Charging Model:

2.5.1 the Director shall inform the Supplier in writing of its reasons for its rejection; and

2.5.2 the Supplier shall then revise the draft Charging Model (taking reasonable account of the Director's comments) and shall re-submit a revised draft Charging Model to the Director for the Director's approval within twenty (20) Working Days of the date of the Director's notice of rejection. The provisions of Paragraph 2.4 and this Paragraph 2.5 shall apply again to any resubmitted draft Charging Model, provided that either Party may refer any disputed matters for resolution by the Charging Model at any time.

2.6 If the Director approves the draft Charging Model, it shall be incorporated into and form part of this Agreement from the date of the Director's notice of approval, provided always that in the event that there is any conflict or inconsistency between the Charging Model and the Pricing Response Template, the Pricing Response Template shall take precedence.

3 APPLICABLE PRICING MECHANISM

3.1 Milestone Payments and Service Charges shall be calculated using the pricing mechanism specified and on the basis of the rates and prices specified in the Charging Model (or, if the Charging Model has not yet been approved by the Director in accordance with Paragraph 2 of this Schedule 7.1 (*Charges and Invoicing),* the Pricing Response Template) as more particularly set out in this Schedule.

3.2 The Charging Model (or, if the Charging Model has not yet been approved by the Director in accordance with Paragraph 2 of this Schedule 7.1 (*Charges and Invoicing),* the Pricing Response Template) sets out which pricing mechanism shall be used to calculate each Milestone Payment, which shall be one or more of the following:

3.2.1 "**Time and Materials**", in which case the provisions of Paragraph 4 shall apply;

3.2.2 "**Firm Price**", in which case the provisions of Paragraph 6 shall apply.

3.3 The Charging Model (or, if the Charging Model has not yet been approved by the Director in accordance with Paragraph 2 of this Schedule 7.1 (*Charges and Invoicing),* the Pricing Response Template) sets out which pricing mechanism shall be used to calculate each Service Charge, which shall be one or more of the following:

3.3.1 "**Time and Materials**", in which case the provisions of Paragraph 4 shall apply; or

3.3.2 "**Volume Based**" pricing, in which case the provisions of Paragraph 7.1.2 shall apply; or

3.3.3 "**Fixed Price**" in which case the provisions of Paragraph 7.1.1 shall apply.

4 TIME AND MATERIALS MILESTONE PAYMENTS OR SERVICE CHARGES

4.1 Where a Change Authorisation Note indicates that a Milestone Payment or Service Charge (as applicable) is to be calculated by reference to a Time and Materials pricing mechanism:

4.1.1 the day rates set out in the relevant section of the Charging Model (or, if the Charging Model has not yet been approved by the Director in accordance with Paragraph 2 of this Schedule 7.1 (*Charges and Invoicing),* Table 6 – Role Based Personnel Rate Card on Tab B5 Pricing of the Pricing Response Template) shall be used to calculate the relevant Charges, provided that the Supplier (or its Sub-contractor) shall:

(a) not be entitled to include any uplift for risks or contingencies within its day rates;

(b) not be paid any Charges to the extent that they would otherwise exceed the cap specified against the relevant Change Authorisation Note unless the Supplier has obtained the Director's prior written consent. The Supplier shall monitor the amount of each Charge incurred in relation to the relevant cap and notify the Director immediately in the event of any risk that the cap may be exceeded and the Director shall instruct the Supplier on how to proceed;

(c) only be entitled to be paid Charges that have been properly and reasonably incurred, taking into account the Supplier's obligation to deliver the Services in a proportionate and efficient manner; and

4.1.2 the Supplier shall keep records of hours properly worked by Supplier Personnel (in the form of timesheets) and expenses incurred and submit a summary of the relevant records with each invoice. If the Director requests copies of such records, the Supplier shall make them available to the Director within ten (10) Working Days of the Director's request.

4.2 The Supplier shall be entitled to Index the rates set out in the relevant section of the Charging Model (or, if the Charging Model has not yet been approved by the Director in accordance with Paragraph 2 of this Schedule 7.1 (*Charges and Invoicing),* Table 6 - Role Based Personnel of the Pricing Response Template), but any caps set out in the relevant section of the Charging Model (or, if the Charging Model has not yet been approved by the Director in accordance with Paragraph 2 of this Schedule 7.1 (*Charges and Invoicing),* Table 6 - Role Based Personnel of the Pricing Response Template) shall not be subject to Indexation.

5 GUARANTEED MAXIMUM PRICE

5.1 Where Change Authorisation Note indicates that a Milestone Payment is to be calculated by reference to a "guaranteed maximum price" pricing mechanism, the costs shall be calculated Time and Materials, in accordance with Paragraph 4 above.

5.2 The maximum Milestone Payment payable by the Director for the relevant Milestone shall not exceed an amount equal to the guaranteed maximum price for that Milestone as identified in the relevant Change Authorisation Note.

6 FIRM PRICE MILESTONE PAYMENTS

6.1 Milestone Payments shall be the Firm Prices set out in the relevant section of the Charging Model (or, if the Charging Model has not yet been approved by the Director in accordance with Paragraph 2 of this Schedule 7.1 (*Charges and Invoicing),* Table 1 Firm Prices Payment Milestones of the Pricing Response Template) as calculated by reference to the relevant section of the Charging Model (or, if the Charging Model has not yet been approved by the Director in accordance with Paragraph 2 of this Schedule 7.1 (*Charges and Invoicing),* B3a Cost Build of the Pricing Response Template).

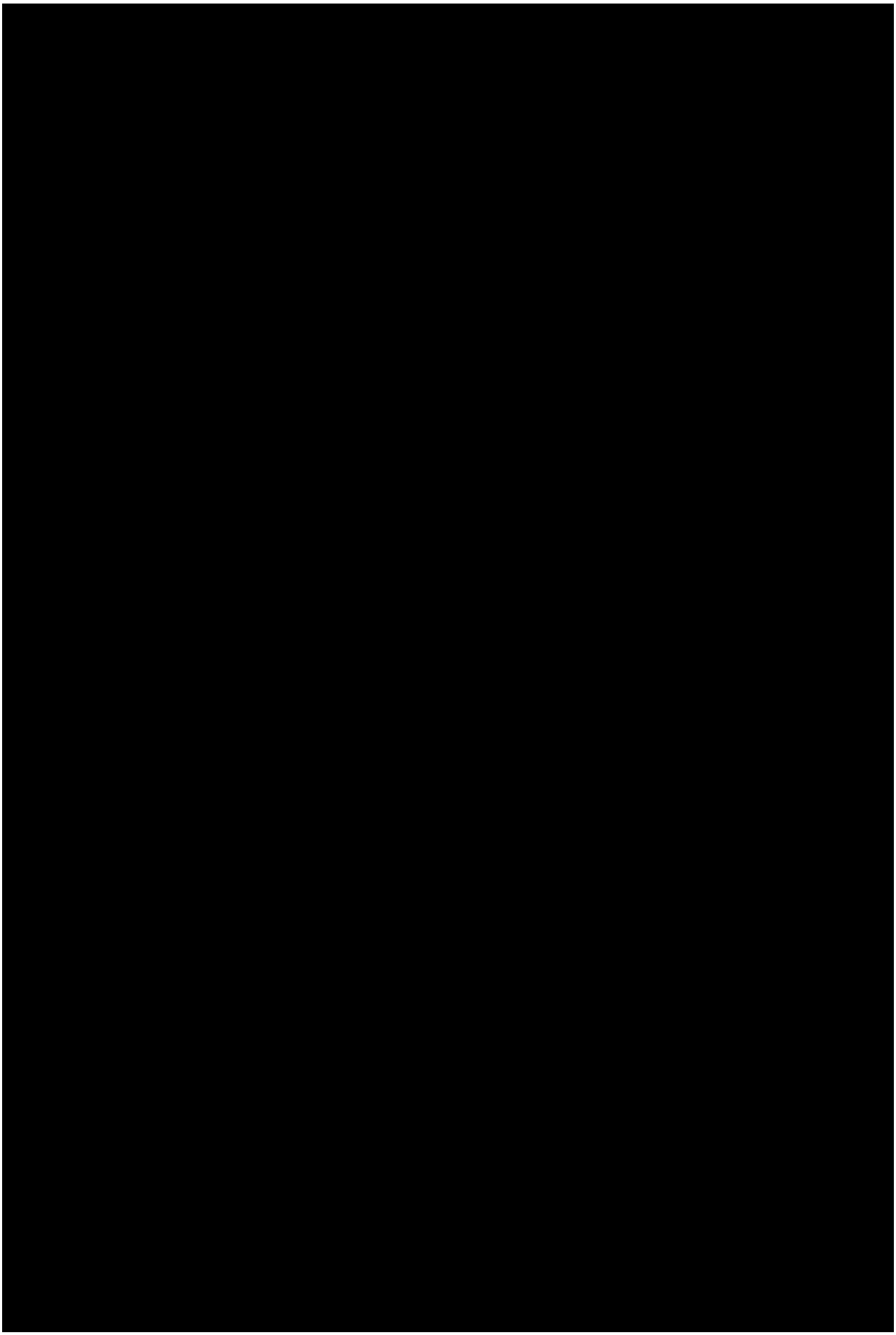
6.2 Charges calculated by reference to a Firm Price pricing mechanism shall not be subject to increase by way of Indexation.

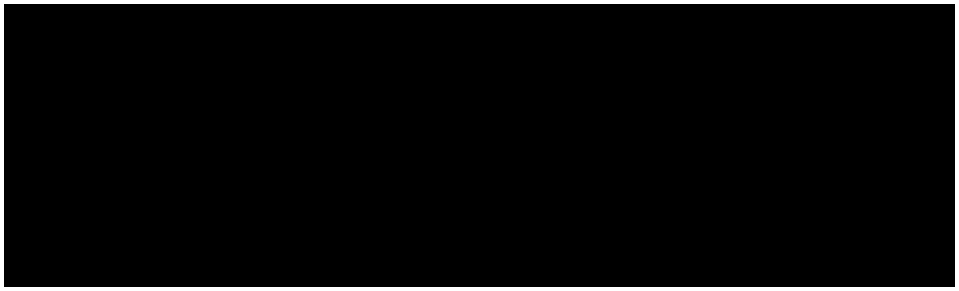
7 SERVICE CHARGES

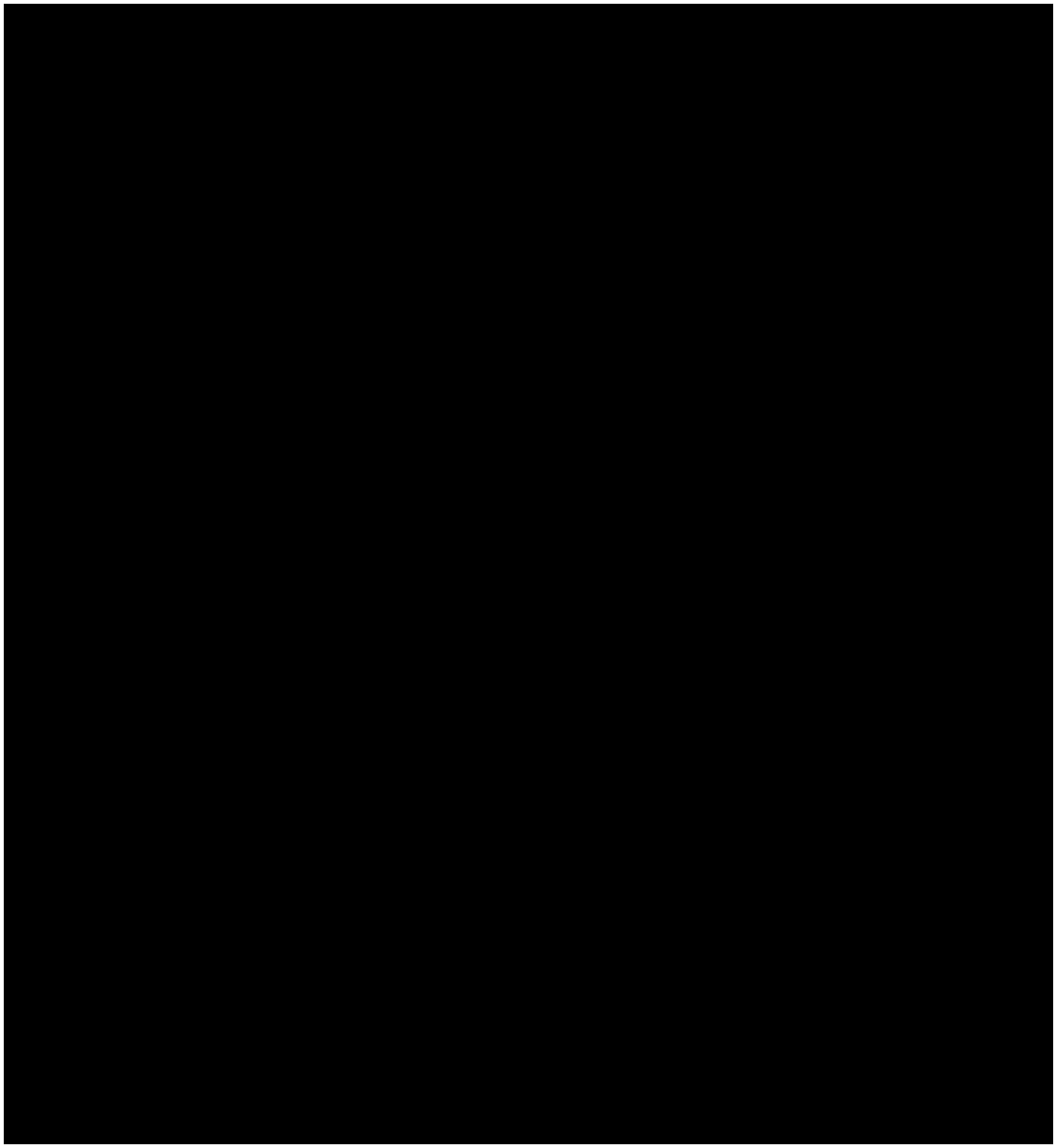
7.1 The Service Charges shall be calculated by reference to:

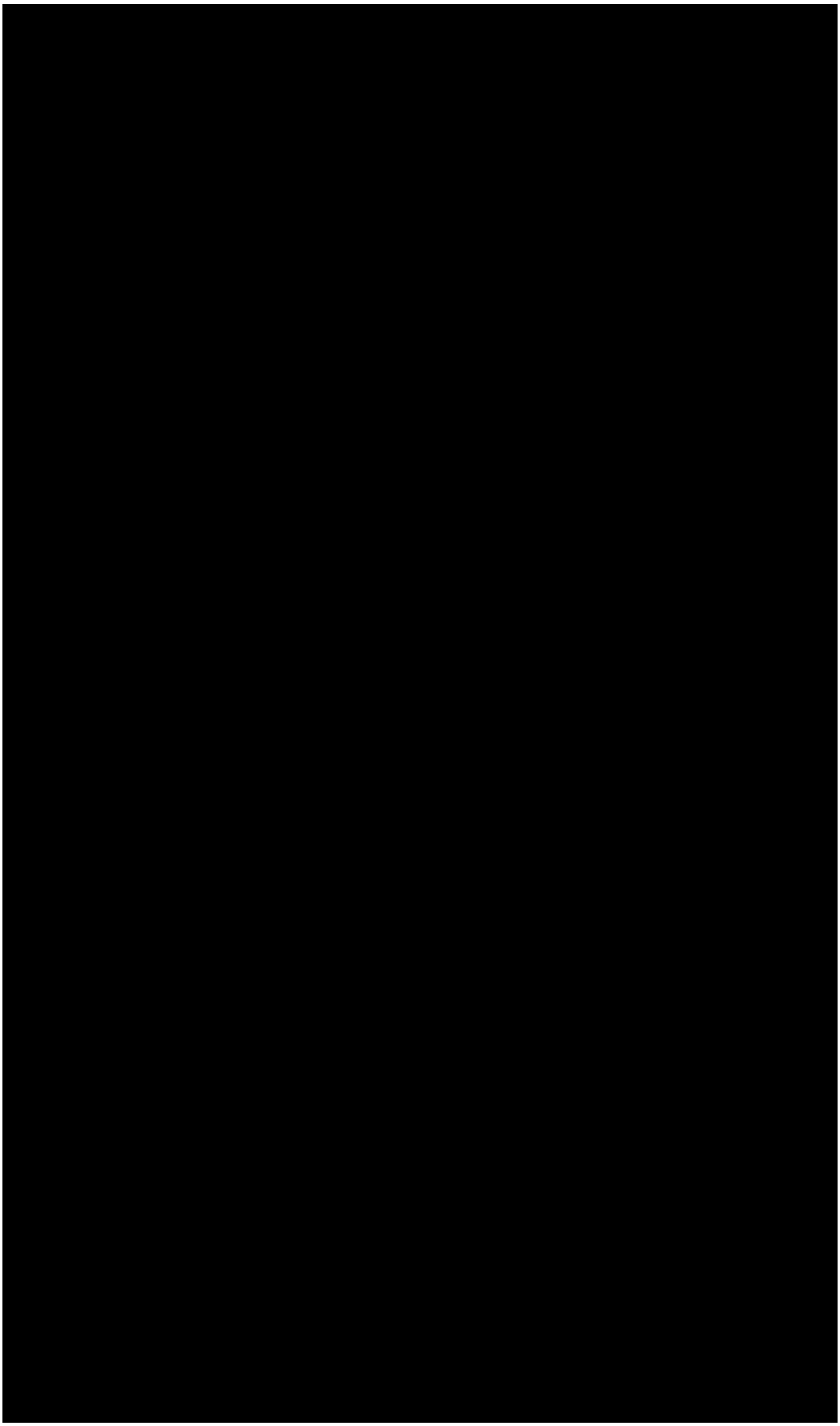
7.1.1 Fixed Price pricing mechanism as set out in the relevant section of the Charging Model (or, if the Charging Model has not yet been approved by the Director in accordance with Paragraph 2 of this Schedule 7.1 (*Charges and Invoicing),* Tables 3 and 5 Fixed Service Charge of the Pricing Response Template), as calculated by reference to the relevant section of the Charging Model (or, if the Charging Model has not yet been approved by the Director in accordance with Paragraph 2 of this Schedule 7.1 (*Charges and Invoicing),* tab B3b Cost Service of the Pricing Response Template); and/or

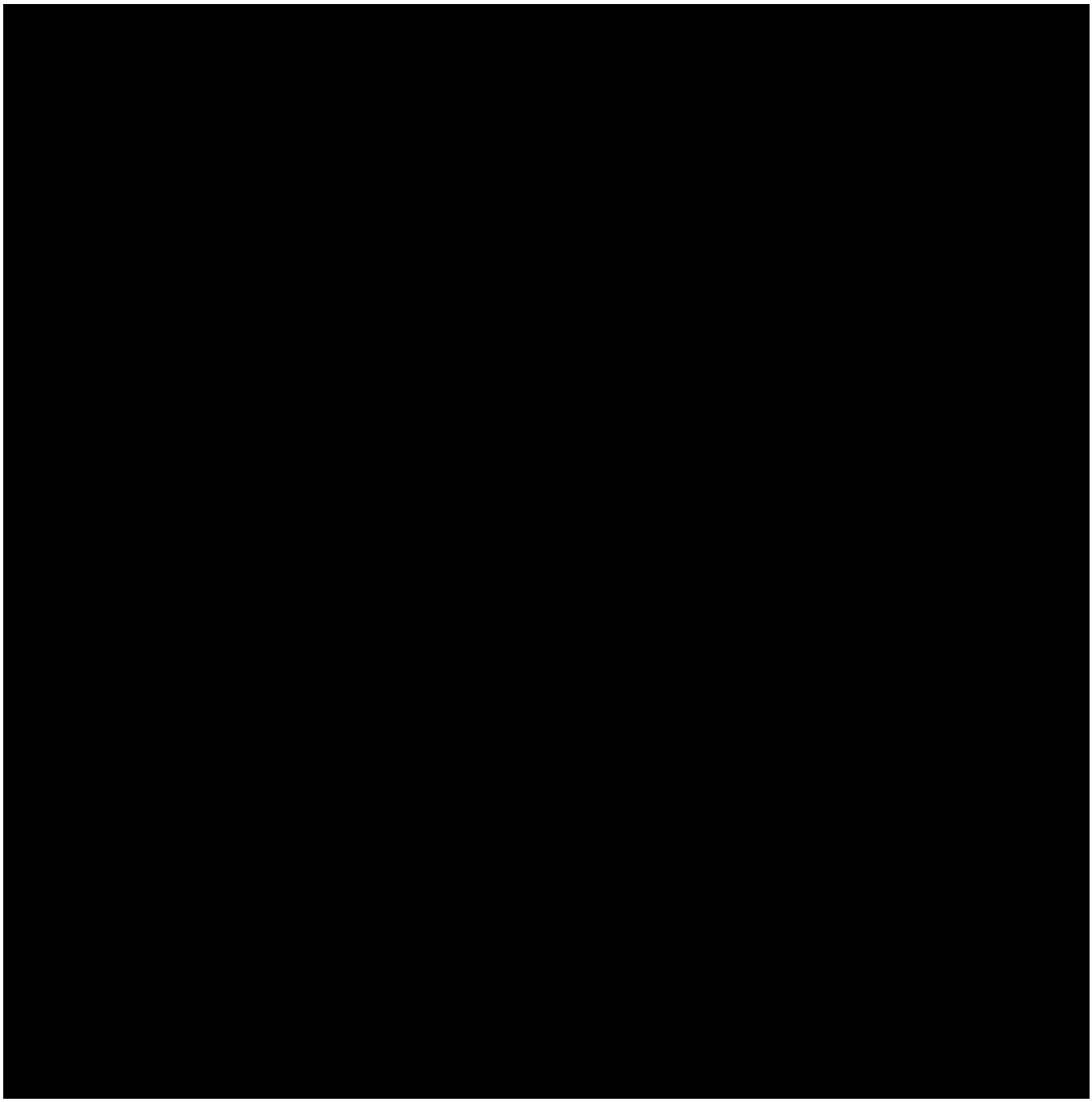
7.1.2 Volume Based pricing mechanism as set out in the relevant section of the Charging Model (or, if the Charging Model has not yet been approved by the Director in accordance with Paragraph 2 of this Schedule 7.1 (*Charges and Invoicing),* Table 4 Volume Based Charges of the Pricing Response Template), as calculated by reference to the relevant section of the Charging Model (or, if the Charging Model has not yet been approved by the Director in accordance with Paragraph 2 of this Schedule 7.1 (*Charges and Invoicing),* B4 Cost Variable of the Pricing Response Template), based on unit costs.











7.2 In the event that the Director elects to extend the Term beyond the Initial Term, the Service Charges for the Extended Period shall, unless otherwise agreed in accordance with Schedule 8.2 (*Change Control Procedure*) be those charges as set out in the Charging Model (or, if the Charging Model has not yet been approved by the Director in accordance with Paragraph 2 of this Schedule 7.1 (*Charges and Invoicing*), the Pricing Response Template) for the final year of the Initial Term as adjusted in accordance with Paragraph 6 of Part 3 (*Indexation).*

8 REIMBURSABLE EXPENSES

8.1 Where:

8.1.1 Services are to be charged using a Time and Materials pricing mechanism; and

8.1.2 the Director so agrees in writing,

the Supplier shall be entitled to be reimbursed by the Director for Reimbursable Expenses (in addition to being paid the relevant Charges), provided that such Reimbursable Expenses are supported by Supporting Documentation.

8.2 The Director shall provide a copy of its current expenses policy to the Supplier upon request.

8.3 Except as expressly set out in Paragraph 8.1, the Charges shall include all costs and expenses relating to the Deliverables, the Services and/or the Supplier's performance of its obligations under this Agreement and no further amounts shall be payable by the Director to the Supplier in respect of such performance, including in respect of matters such as:

8.3.1 any incidental expenses that the Supplier incurs, including travel, subsistence and lodging, document and report reproduction, shipping, desktop and office equipment costs required by the Supplier Personnel, including network or data interchange costs or other telecommunications charges; or

8.3.2 any amount for any services provided or costs incurred by the Supplier prior to the Effective Date.

9 PASS THROUGH ITEMS

9.1 Pass Through Items shall include:

9.1.1 purchases of ad-hoc hardware, Software and other goods and services to the Director's specification which are to be used in delivering the Services;

9.1.2 purchases in relation to the subject matter of this Agreement requested by the Director, procured on behalf of the Director for the benefit of the Director, which meet the following criteria:

(a) are for the Director's own use and are not required to enable the Supplier to deliver the Services;

(b) use the Director-provided business specification (and so are provided via the Supplier but at the Director's risk, if the purchased goods or services do not work/operate as expected); and

(c) utilise an existing contract for similar products or services owned by the Supplier subject to the supplier under that contract agrees to such use of the existing contract.

9.2 The Supplier shall charge the Director at cost for the Pass Through Items. No element of the Supplier Profit Margin or any other charges may be added to the cost of Pass Through Items.

9.3 The Supplier shall pass on to the Director the benefit of any discounts or rebates that it obtained in purchasing the Pass Through Items or through any general marketing or strategic relationship between the Supplier and the relevant provider of goods or services. Where a Subsidiary Undertaking of the Supplier manufactures the Pass Through Items, the Supplier shall pass on to the Director the benefit of any discounts or rebates that it obtains from the Subsidiary Undertaking in purchasing the Pass Through Items. Where the Supplier and the Subsidiary Undertaking both manufacture the Pass Through Items, the margin and overhead treatment applied to the Pass Through Items manufactured by the Subsidiary Undertaking shall also apply to the Pass Through Items manufactured by the Supplier.

10 PASS THROUGH ITEMS (SUPPLIER ACTING AS AGENT)

10.1 Pass Through Items (Supplier Acting As Agent) shall include purchases of the following types of services from Sub-contractors to the Director's specification which are to be used in delivering the Services:

10.1.1 Postal charges including inbound, outbound and mail redirection; and

10.1.2 inbound telephony charges.

10.2 Where the Supplier engages a Sub-contractor to deliver Pass Through Items (Supplier Acting As Agent), such Sub-contractor shall be deemed to be the principal provider of such items under this Agreement.

10.3 The Supplier shall charge the Director at cost for the Pass Through Items (Supplier Acting As Agent). No element of the Supplier and/or Sub-contractor Profit Margin or any other charges may be added to the cost of the Pass Through Items (Supplier Acting As Agent).

10.4 The Supplier shall pass on to the Director the benefit of any discounts or rebates that it obtained in purchasing the Pass Through Items (Supplier Acting As Agent) or through any general marketing or strategic relationship between the Supplier and/or the Sub-contractor and the relevant third party provider of goods or services.

10.5 The Supplier shall forward the invoice received from the relevant Sub-contractor without amendment and in accordance with the invoice requirements in Part 5 within five (5) Working Days of it being received from the original provider and the Director shall (subject only to the correction of any mathematical errors or valid dispute) pay the Supplier the total amount of the invoice within twenty (20) days of receipt of the invoice. These sums shall be treated as Charges for the purpose of Clause 10.3 but not otherwise. The Supplier shall mark such invoices as "**URGENT – Payment of Pass-through**".

10.6 Pass Through Items (Supplier Acting As Agent) shall not be subject to Indexation (according to Part 3 Adjustments to the Charges, Paragraph 6 of this Schedule). Instead the charge for the items shall be that levied by the original Sub-contractor that is applicable at the time the items are provided.

PART 2: CHARGING MECHANISMS

1 MILESTONE PAYMENTS

1.1 On the Achievement of a Milestone the Supplier shall be entitled to invoice the Director for the Milestone Payment associated with that Milestone, as specified in the Charging Model (or, if the Charging Model has not yet been approved by the Director in accordance with Paragraph 2 of this Schedule 7.1 (*Charges and Invoicing*), Table 1 Firm Prices Milestone Payments of the Pricing Response Template) (or as otherwise identified in a Change Authorisation Note).

1.2 Each invoice relating to a Milestone Payment shall be supported by:

1.2.1 a Milestone Achievement Certificate; and

1.2.2 where the Milestone Payment is to be calculated by reference to Time and Materials or a Guaranteed Maximum Price, a Certificate of Costs with Supporting Documentation.

1.3 Subject to Paragraph 1.4 of this Part 2, the Supplier shall issue all invoices within three (3) months of the date of the Milestone Achievement Certificate for the relevant Milestone. Any invoice issued after this period shall be deemed invalid.

1.4 If the Supplier believes exceptional circumstances exist which will prevent it from being able to issue an invoice to the Director within the relevant period specified in Paragraph 1.3 of Part 2, the Supplier shall, prior to expiry of this period, notify the Director in writing of this fact and set out the reasons why it is unable to issue the invoice. Following receipt of this notification, the Director may agree to extend the period during which this invoice can be issued.

2 SERVICE CHARGES

2.1 On the Achievement of:

2.1.1 the first Operational Services Commencement Date (OSCD 1 Milestone), the Service Charge for the relevant part of the Operational Services shall commence;

2.1.2 the first Operational Services Commencement Date (OSCD 1 Milestone) the Charge for the Development Pool shall commence; and

2.1.3 the subsequent Operational Service Commencement Date Milestones, the Services Charge for the relevant remaining part of the Operational Services shall commence.

2.2 Service Charges shall be invoiced by the Supplier for each Service Period monthly in arrears in accordance with the requirements of Part 5 within ten (10) Working Days of the last day of the Service Period in question.

2.3 If a Service Charge is to be calculated by reference to a Fixed Price pricing mechanism and the relevant Service:

2.3.1 commences on a day other than the first day of a month; and/or

2.3.2 ends on a day other than the last day of a month,

the Service Charge for the relevant Service Period shall be pro-rated based on the proportion which the number of days in the month for which the Service is provided bears to the total number of days in that month.

2.4 Any Service Credits that accrue during a Service Period shall be deducted from the Service Charges payable for the next following Service Period. An invoice for a Service Charge shall not be payable by

the Director unless all adjustments (including Service Credits and Compensation Credits, if any) relating to the Service Charges for the immediately preceding Service Period have been agreed.

3 ADDITIONAL SERVICES

3.1 If the Director gives notice pursuant to Clause 5.11 (*Additional Services*) that it requires the Supplier to provide any or all of the Additional Services:

3.1.1 the Milestone Payments (if any) for the relevant Additional Services shall be calculated either by reference to:

(a) the pricing mechanism for those Additional Services set out in Table 2 or such other relevant part of the Pricing Response Template including Table 6 (Bidder Role Rate Card) of the Pricing Response Template as calculated by reference to Tabs B1a and B1b of the Pricing Response Template; or

(b) where such Additional Services are not expressly priced in the Pricing Response Template, based on the pricing information and methodology used to calculate the Charges pursuant to the Pricing Response Template; and

3.1.2 the Charges for the relevant Additional Services shall where it relates to the Services shall form part of the Service Charge to be calculated in accordance with:

(a) Paragraph 2 of Part 2 (*Charging Mechanisms*) above; or otherwise

(b) by reference to tab B3a Cost Service of the Pricing Response Template,

and in all cases as set out in the relevant Change Authorisation Note and/or the Agreement Amendment pursuant to Schedule 8.2 (*Change Control Process*).

4 COLLABORATION REWARD POT

4.1 The Director, at its sole discretion shall be entitled to determine the value of the Reward Pot, to be awarded pursuant to the terms of the Collaboration Agreement, each year at it sole discretion and shall use the Universal Standard Charge accordingly.

4.2 The Supplier shall be entitled to invoice the Director for the amount of the Reward Pot, awarded to it by the Director pursuant to the terms of the Collaboration Agreement.

PART 3: ADJUSTMENTS TO THE CHARGES

1 NOT USED

2 PAYMENTS FOR DELAYS DUE TO DIRECTOR CAUSE

2.1 If the Supplier is entitled in accordance with Clause 33.1.3(c)(iii) (*Director Cause*) to compensation for failure to Achieve a Milestone by its Milestone Date, then, subject always to Clause 27 (*Limitations on Liability*), such compensation shall be determined in accordance with the following principles:

2.1.1 the compensation shall reimburse the Supplier for additional Costs incurred by the Supplier that the Supplier:

(a) can demonstrate it has incurred solely and directly as a result of the Director Cause; and

(b) is, has been, or will be unable to mitigate, having complied with its obligations under Clause 33.1 (*Director Cause*),

together with an amount equal to the Anticipated Contract Life Profit Margin thereon; and

2.1.2 the compensation shall not operate so as to put the Supplier in a better position than it would have been in but for the occurrence of the Director Cause.

2.2 The Supplier shall provide the Director with any information the Director may require in order to assess the validity of the Supplier's claim to compensation.

3 SERVICE CREDITS

3.1 Service Credits shall be calculated by reference to the number of Service Points accrued in any one Service Period pursuant to the provisions of Schedule 2.2 (*Performance Levels*).

3.2 For each Service Period:

3.2.1 the Service Points accrued shall be converted to a percentage deduction from the Service Charges for the relevant Service Period on the basis of one point equating to a 0.042% deduction in the Service Charges; and

3.2.2 the total Service Credits applicable for the Service Period shall be calculated in accordance with the following formula:

$$SC = TSP \times x \times AC$$

where:

SC is the total Service Credits for the relevant Service Period;

TSP is the total Service Points that have accrued for the relevant Service Period;

X is [redacted]; and

AC is the total Services Charges payable for the relevant Service Period (prior to deduction of applicable Service Credits).

3.3 The liability of the Supplier in respect of Service Credits shall be subject to Clause 27.4.3 (*Financial and other limits*) provided that, for the avoidance of doubt, the operation of the Service Credit Cap

shall not affect the continued accrual of Service Points in excess of such financial limit in accordance with the provisions of Schedule 2.2 (*Performance Levels*).

3.4 Service Credits are a reduction of the Service Charges payable in respect of the relevant Services to reflect the reduced value of the Services actually received and are stated exclusive of VAT.

3.5 Service Credits shall be shown as a deduction from the amount due from the Director to the Supplier in the invoice for the Service Period immediately succeeding the Service Period to which they relate.

4 COMPENSATION AND GOODWILL PAYMENTS

4.1 Compensation and Goodwill Payments shall be managed centrally by the Supplier on behalf of the Director, subject always to the Director's Compensation and Goodwill Policy.

4.2 The Supplier shall, on the basis of the information provided by the Customer and always in accordance with the Director's Compensation and Goodwill Policy, make payment to the relevant Customer(s) in respect of applicable Compensation and Goodwill Payments accrued during the relevant Service Period.

4.3 Following payment of the Compensation and Goodwill Payments under Paragraph 4.2, the Supplier shall prepare and issue to the Director a report detailing all relevant (at the discretion of the Director) Compensation and Goodwill Payments made in the relevant Service Period (the "**Compensation and Goodwill Payments Report**") as soon as reasonably possible after the last day of the Service Period in question. Following agreement of the contents of the Compensation and Goodwill Payments Report, the Director shall circulate the Compensation and Goodwill Payments Report (or applicable part thereof) to the Relevant Third Party Suppliers.

4.4 The Compensation and Goodwill Payments Report shall include:

4.4.1 the quantum of each Payment made;

4.4.2 subject to confidentiality and Data Protection Obligations, details of the associated complaint, including where possible a root cause; and

4.4.3 the Supplier's determination of responsibility (and therefore liability for the applicable Compensation Credits), based on the information available, for the failure of performance or other primary contributing factor which gave rise to the complaint.

4.5 Compensation Credits shall be calculated by reference to that proportion of the amount paid by the Supplier to Customers which is attributable to the Services provided by the Supplier as determined in accordance with Paragraph 4.2 above in any one Service Period. For the avoidance of doubt, Compensation Credits may be attributable to the Supplier itself and in such circumstances the Supplier shall not be entitled to recover the Compensation Credits attributable to its own Services.

4.6 Notwithstanding Paragraph 4.5, the Supplier may on the basis of the agreed Compensation and Goodwill Payments Report for the relevant Service Period issue an invoice to the Director in respect of the Compensation Credits attributable to any other Relevant Third Party Supplier during that Service Period.

4.7 If any Relevant Third Party Supplier wishes to appeal any determination in respect of Compensation Credits from the previous Service Period's Compensation and Goodwill Payments Report, it must in the first instance seek to resolve the matter directly with the Supplier, in accordance with the principles under the Collaboration Agreement. Unless explicitly agreed otherwise in writing by the Director, appeals relating to determinations in respect of Compensation Credits shall have no recourse to the Dispute Resolution Procedure, and the appeals process under this Paragraph 4.7 and Paragraph 4.8 shall be the exclusive process for resolving such disputes.

4.8 If the Relevant Third Party Supplier is not satisfied with the outcome of the appeal process in Paragraph 4.7, it may escalate the matter to the Director. The Director shall have ultimate authority in such circumstances and its determination on the liability for such Compensation Credits (and therefore

the responsibility for resolving any underlying cause giving rise to the associated Compensation and Goodwill Payment) shall be final and binding.

4.9 The Director shall provide the Supplier with reasonable assistance and access to information within its possession or reasonable control in relation to any Compensation and Goodwill Payments and which the Director deems is relevant to the Compensation Credit being claimed.

4.10 The liability of the Supplier in respect of Compensation Credits shall be subject to Clause 27.4.4 (*Financial and other limits*).

5 CHANGES TO CHARGES

5.1 Any Changes to the Charges shall be developed and agreed by the Parties in accordance with Schedule 8.2 (*Change Control Procedure*) and on the basis that the Supplier Profit Margin on such Charges shall:

5.1.1 be no greater than that applying to Charges using the same pricing mechanism as at the Effective Date (as set out in the Contract Inception Report); and

5.1.2 in no event exceed the Maximum Permitted Profit Margin.

5.2 The Director may request that any Impact Assessment presents Charges without Indexation for the purposes of comparison.

6 INDEXATION

6.1 Any amounts or sums in this Agreement which are expressed to be "subject to Indexation" shall be adjusted in accordance with the provisions of this Paragraph 6 to reflect the effects of inflation.

6.2 Where Indexation applies, the relevant adjustment shall be:

6.2.1 applied on the 1st April 2024 and on the first day of April in each subsequent year (each such date an "**Adjustment Date**"); and

6.2.2 determined by multiplying the relevant amount or sum by the percentage increase or changes in the Consumer Price Index published in February for the twelve (12) months ended on the thirty-first (31st) of January immediately preceding the relevant Adjustment Date. The value of the index for February 2023 shall be used as the baseline value of the index.

6.3 The indexed Charge shall be calculated in accordance with the following formula:

$$AD_a = AD_1 \times \frac{Index_o}{Index_d}$$

Where

AD_a = new indexed Charge

AD_1 = the Charge as stated in this Schedule as at the Effective Date

"$Index_o$" = the value of the relevant published index for the February immediately preceding the current Financial Year

"$Index_d$" = the value of relevant published index for February 2023.

6.4 Except as set out in this Paragraph 6, neither the Charges nor any other costs, expenses, fees or charges shall be adjusted to take account of any inflation, change to exchange rate, change to interest

rate or any other factor or element which might otherwise increase the cost to the Supplier or Sub-contractors of the performance of their obligations.

7 ALLOWABLE ASSUMPTIONS

7.1 The Supplier shall determine whether each Allowable Assumption is accurate within its Verification Period.

7.2 During each Verification Period, the Director shall provide the Supplier with reasonable assistance and access to information within its possession or reasonable control and which the Director deems is relevant to the Allowable Assumption being verified.

7.3 No later than ten (10) Working Days after the end of each Verification Period, the Supplier shall provide the Director with a written report setting out the results of the Supplier's verification activity for the relevant Allowable Assumption, including whether the Allowable Assumption is accurate or whether the Implementation Plan and/or the Contract Inception Report require adjustment.

7.4 Each Allowable Assumption shall be deemed accurate unless adjusting for the relevant Allowable Assumption has an impact:

7.4.1 on tab B5_Pricing tab of the Pricing Response Template; or

7.4.2 on the Implementation Plan which would require adjustment under the Change Control Procedure, as identified at tab B2a or B2b of the Pricing Response Template,

in which case Paragraph 7.5 shall apply.

7.5 Where the Parties agree that an Allowable Assumption is not accurate and the Pricing Response Table and/or Implementation Plan require adjusting:

7.5.1 the Supplier shall take all reasonable steps to mitigate the impact of the Allowable Assumption on the Financial Model and/or the Implementation Plan including those mitigations set out in against the relevant Allowable Assumption;

7.5.2 the Supplier may (subject to Paragraph 7.5.3) propose a Change to take account of the impact of the adjustment of the Allowable Assumption and such Change Request shall be considered in accordance with the Change Control Procedure notwithstanding Paragraphs 5.1.7, 7.5, 10.5, 11.1.2 and 11.3 of Schedule 8.2 (*Change Control Procedure*) the Director shall not unreasonably delay or reject such Change Request, nor, following approval, unreasonably delay or refuse to issue the resulting Change Authorisation Note; and

7.5.3 where the Supplier proposes a Change to the Charges under Paragraph 7.5.2, the Change Request shall reflect the details of the applicable Allowable Assumption in tabs B3a or B3b of the Pricing Response Template, including the requirement that any proposed adjustment to the Charges shall not exceed the maximum impact on the relevant Charges as specified in “Total Allocated” column of tabs B2a or B2b of the Pricing Response Template.

8 VOLUME FORECASTING

8.1 Commencing three (3) months prior to the first Operational Service Commencement Date and each month thereafter during the Term, the Parties shall meet (which meeting may be conducted using remote meeting tools) to discuss the expected future evolution of the quantity (volume) received for each category of Customer input to the Service as set out in the Excel spreadsheet entitled Lot1 – Appendix 9 – ISFT Volumetrics (which is reproduced in Annex 3 of this Schedule 7.1) in Table 1 entitled ‘12 month projection of volumes for 2023' in column A.

8.2 During each meeting the Supplier shall present its view of the expected numerical evolution in each category for the next twelve (12) months taking into account seasonality and past trends and the Director will present any business initiatives or factors that it anticipates may have an impact on the

expected volume evolution during the same period. The Supplier will consider and make suitable adjustments to the forecast based on the input of both Parties during the meeting.

8.3 Following each meeting a report detailing the forecast and historical actual volumes against each category of Customer input for the following twelve (12) months (the forecast period) and the previous twelve (12) months (the past history) shall be produced by the Supplier and provided to the Director within five (5) Working Days of the meeting taking place.

8.4 Each report shall be reviewed at the next monthly Supplier Delivery and Supplier Management Committee meeting following the submission of the report.

8.5 The Director accepts and agrees that past history information presented prior to the completion of Milestone MS13 (the third Operational Service Commencement Date) will include information that has been obtained from the Former Supplier which may be incomplete or inaccurate.

8.6 If the Parties see a sustained increase or decrease in the volumes as set out in the Baseline Volumes in Appendix 2 above, over a period of time, the parties will discuss if any adjustments are required. Any adjustments shall be considered in accordance with the Change Control Procedure.

8.7 The Parties shall carry out an annual review to consider the group of the processes and any re-profiling of the volumes over the year and against each process. If the output of that annual review requires a change to the baseline volumes or the forecast for future years and/or the Charging Model, any such Change shall be carried out in accordance with the Change Control Procedure.

PART 4: EXCESSIVE SUPPLIER PROFIT MARGIN

1 LIMIT ON SUPPLIER PROFIT MARGIN IN THE PRICING RESPONSE TEMPLATE

1.1 The Supplier acknowledges that the Achieved Profit Margin applicable over the Term shall not exceed the Maximum Permitted Profit Margin.

1.2 The Supplier shall include in each Annual Contract Report the Achieved Profit Margin as at the end of the Contract Year to which the Annual Contract Report is made up and the provisions of Paragraph 2 of Part 2 of Schedule 7.5 (*Financial Reports and Audit Rights*) shall apply to the approval of the Annual Contract Report.

2 ADJUSTMENT TO THE CHARGES IN THE EVENT OF EXCESS SUPPLIER PROFIT

2.1 If an Annual Contract Report demonstrates (or it is otherwise determined pursuant to Paragraph 2 of Part 2 of Schedule 7.5 (*Financial Reports and Audit Rights*)) that the Achieved Profit Margin as at the end of the Contract Year to which the Annual Contract Report is made up exceeds the Maximum Permitted Profit Margin:

2.1.1 the Supplier shall, within five (5) Working Days of delivery to the Director of the Annual Contract Report, propose such adjustments to the Charges as will ensure that the Achieved Profit Margin both over the Contract Year to which the next Annual Contract Report will relate and over the Term will not exceed the Maximum Permitted Profit Margin;

2.1.2 the Director (acting reasonably) may agree or reject the proposed adjustments;

2.1.3 if the Director rejects the proposed adjustments it shall give reasons and the Supplier shall propose revised adjustments within ten (10) Working Days of receiving those reasons; and

2.1.4 if the Parties cannot agree such revised adjustments and the Director terminates this Agreement by issuing a Termination Notice to the Supplier pursuant to Clause 35.1 (*Termination by the Director*), then for the purpose of calculating any Compensation Payment due to the Supplier, the Termination Notice shall be deemed to have been served as at the date of receipt by the Director of the relevant Annual Contract Report.

2.2 Pending agreement of a proposed adjustment to the Charges pursuant to this Part 4, the Charges then in force shall continue to apply. Once the adjustments to the Charges are agreed in accordance with Paragraph 2.1, the Parties shall document the adjustment in a Change Authorisation Note and the adjusted Charges shall apply with effect from the first day of the Service Period that immediately follows the Service Period in which the Change Authorisation Note is executed or such other date as is specified in the Change Authorisation Note.

PART 5: INVOICING AND PAYMENT TERMS

1 SUPPLIER INVOICES

1.1 The Director shall accept for processing any electronic invoice that complies with the Electronic Invoicing Guidance (VAT Notice 700/63) published by HM Revenue & Customs, provided that it is valid and undisputed.

1.2 If the Supplier proposes to submit for payment an invoice that does not comply with the Electronic Invoicing Guidance (VAT Notice 700/63) the Supplier shall:

1.2.1 comply with the requirements of the Director's e-invoicing system;

1.2.2 prepare and provide to the Director for approval of the format a template invoice and any necessary Supporting Documentation within ten (10) Working Days of the Effective Date which shall include, as a minimum the details set out in Paragraph 1.3 together with such other information as the Director may reasonably require to assess whether the Charges that will be detailed therein are properly payable; and

1.2.3 make such amendments as may be reasonably required by the Director if the template invoice outlined in Paragraph 1.2.2 is not approved by the Director.

1.3 The Supplier shall ensure that each invoice is submitted in the correct format for the Director's e-invoicing system, or that it (or, if the format of the invoice does not accommodate the necessary information, any accompanying Supporting Documentation) contains the following information:

1.3.1 the date of the invoice;

1.3.2 a unique invoice number;

1.3.3 the Service Period or other period(s) to which the relevant Charge(s) relate;

1.3.4 the correct reference for this Agreement;

1.3.5 the reference number of the purchase order to which it relates (if any);

1.3.6 the dates between which the Services subject of each of the Charges detailed on the invoice were performed;

1.3.7 a description of the Services;

1.3.8 the pricing mechanism used to calculate the Charges (Milestone Payment, Fixed Price, Volume Based ("**Variable Price**") or Time and Materials);

1.3.9 any payments due in respect of Achievement of a Milestone, including the Milestone Achievement Certificate number for each relevant Milestone;

1.3.10 the total Charges gross and net of any applicable deductions and, separately, the amount of any Reimbursable Expenses properly chargeable to the Director under the terms of this Agreement, and, separately, any VAT or other sales tax payable in respect of each of the same;

1.3.11 where applicable, an itemised list of costs incurred in respect of any B2B Service (if any);

1.3.12 details of any Service Credits or similar deductions that shall apply to the Charges detailed on the invoice;

1.3.13 any amounts outstanding from previous invoices;

1.3.14 reference to any reports required by the Director in respect of the Services to which the Charges detailed on the invoice relate (or in the case of reports issued by the Supplier for validation by the Director, then to any such reports as are validated by the Director in respect of the Services), including but not limited to the volumes used to calculate the Variable Price element of the Service Charges;

1.3.15 a contact name and telephone number of a responsible person in the Supplier's finance department in the event of administrative queries;

1.3.16 the banking details for payment to the Supplier via electronic transfer of funds (i.e. name and address of bank, sort code, account name and number); and

1.3.17 where the Services have been structured into separate Service lines, the information at 1.3.1 to 1.3.16 of this Paragraph 1.3 shall be broken down in each invoice per Service line.

1.4 The Supplier shall invoice the Director in respect of Services in accordance with the requirements of Part 2. The Supplier shall first submit to the Director a draft invoice setting out the Charges payable. The Parties shall endeavour to agree the draft invoice within five (5) Working Days of its receipt by the Director, following which the Supplier shall be entitled to submit its invoice.

1.5 Each invoice shall at all times be accompanied by and submitted with Supporting Documentation. Any assessment by the Director as to what constitutes Supporting Documentation shall not be conclusive and the Supplier undertakes to provide to the Director any other documentation reasonably required by the Director from time to time to substantiate an invoice.

1.6 Unless notified otherwise in writing by the Director, the Supplier shall submit all invoices and Supporting Documentation in accordance with this Schedule by email to *Accounts.Payable@nsandi.com*, with invoices addressed to:

Accounts Payable

NS&I
Sanctuary Buildings
20 Great Smith Street
London
SW1P 3BT,

with a copy (again including any Supporting Documentation) to such other person and at such place as the Director may notify to the Supplier from time to time.

1.7 All Supplier invoices shall be expressed in sterling or such other currency as shall be permitted by the Director in writing.

1.8 The Director shall regard an invoice as valid only if it complies with the provisions of this Part 5. Where any invoice does not conform to the Director's requirements set out in this Part 5, the Director shall promptly return the disputed invoice to the Supplier and the Supplier shall promptly issue a replacement invoice which shall comply with such requirements.

1.9 If the Director fails to consider and verify an invoice in accordance with Paragraphs 1.4 and 1.8, the invoice shall be regarded as valid and undisputed for the purpose of Paragraph 2.1 and payment shall be considered due thirty (30) days after a reasonable time has passed.

2 PAYMENT TERMS

2.1 Subject to the relevant provisions of this Schedule, the Director shall make payment to the Supplier within thirty (30) days of verifying that the invoice is valid and undisputed.

2.2 Unless the Parties agree otherwise in writing, all Supplier invoices shall be paid in sterling by electronic transfer of funds to the bank account that the Supplier has specified on its invoice. If the Director

withholds payment or part payment of an invoice, it shall promptly notify the Supplier, with an explanation of the withheld payment.

ANNEX 1: PRICING RESPONSE TEMPLATE

17.1 Annex 1 Schedule 7.1 Pricing Response Template (48635581.1).xlsx

The Pricing Response Template contained in the Excel File reference "*17.1 Annex 1 Schedule 7.1 Pricing Response Template*".

ANNEX 2: PRO-FORMA CERTIFICATE OF COSTS

I [***name of CFO or Director of Finance or equivalent as agreed in advance in writing with the Director]*** of ***[insert name of Supplier***], certify that the financial information provided as part of this Certificate of Costs, incurred in relation to the [***insert name/reference for the Agreement***] (the "**Agreement**") in relation to the following Milestone:

[***Insert details of Milestone***]

1 has been reasonably and properly incurred in accordance with [***name of Supplier***]'s books, accounts, other documents and records;

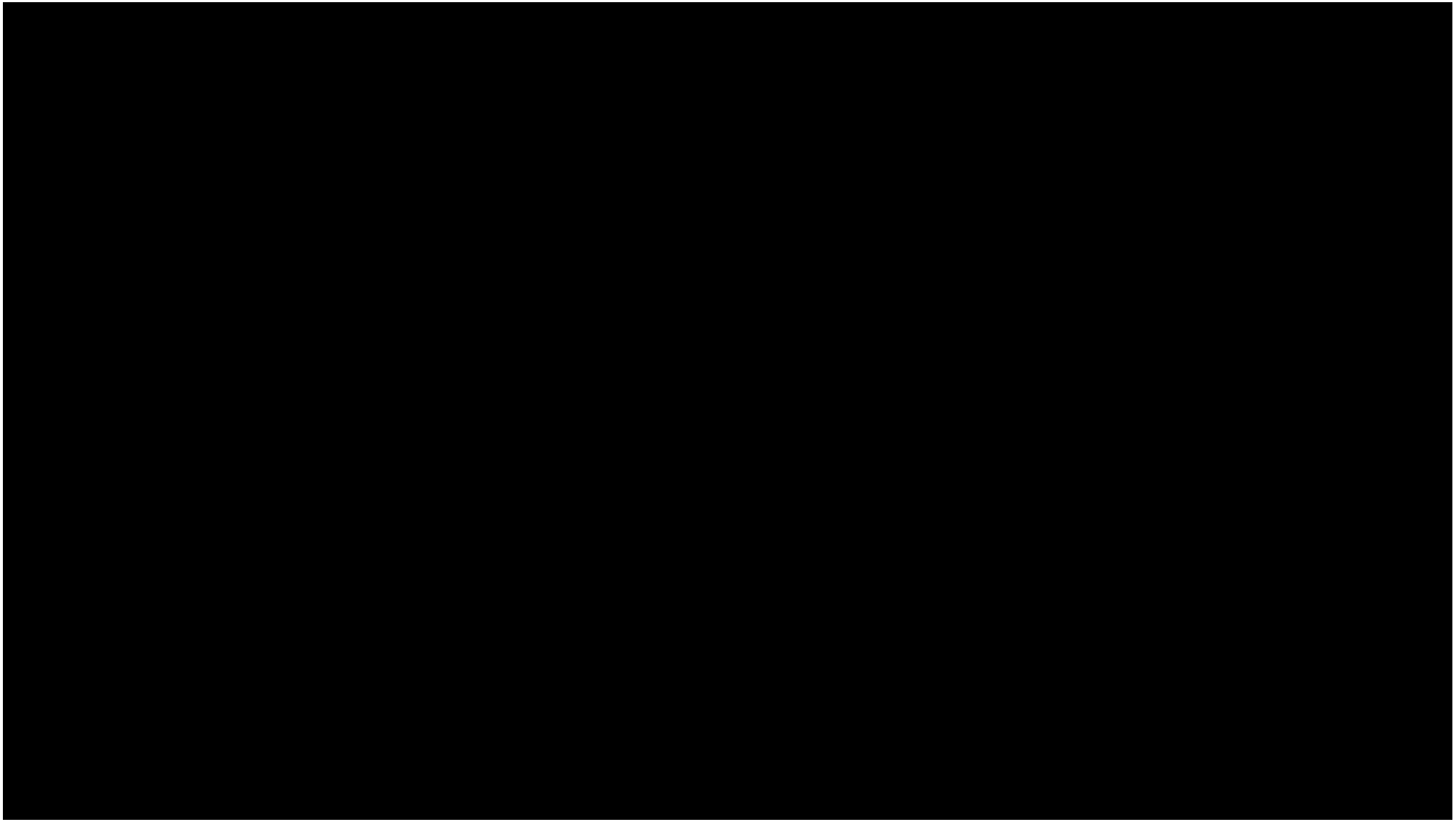
2 is accurate and not misleading in all key respects; and

3 is in conformity with the Agreement and with all generally accepted accounting principles within the United Kingdom.

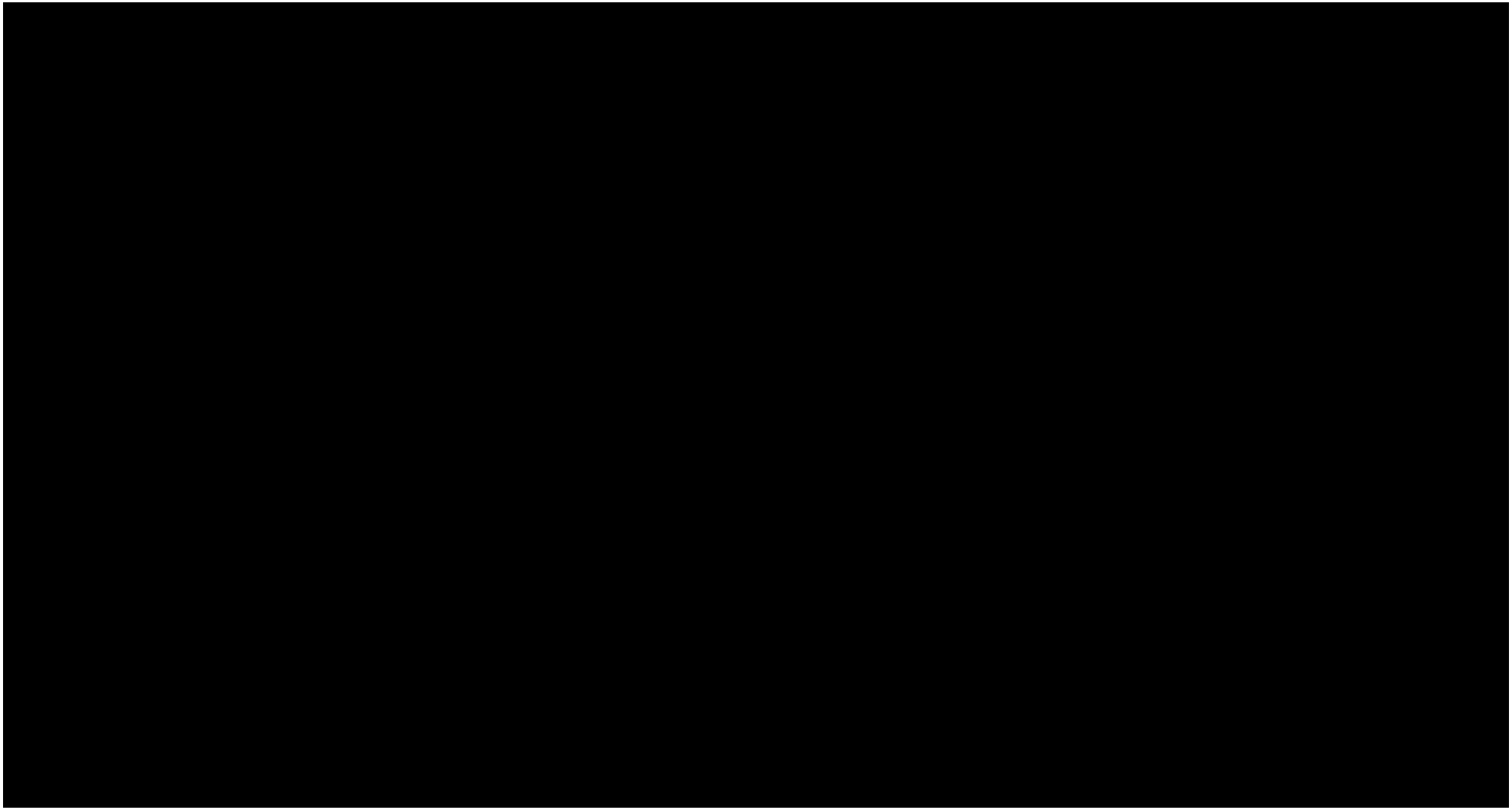
Signed [***Director of Finance or equivalent***]

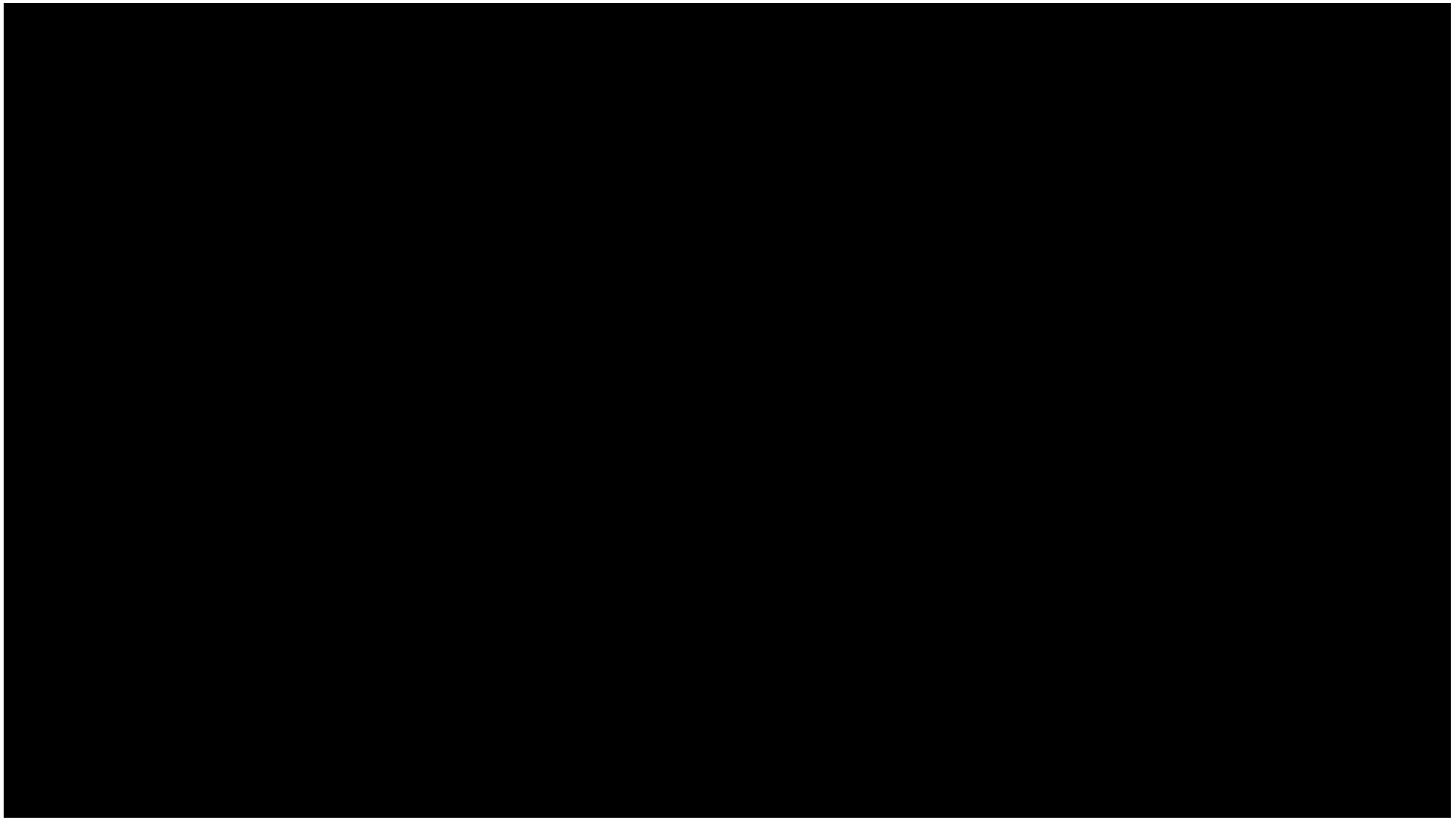
[***Name of Supplier***]

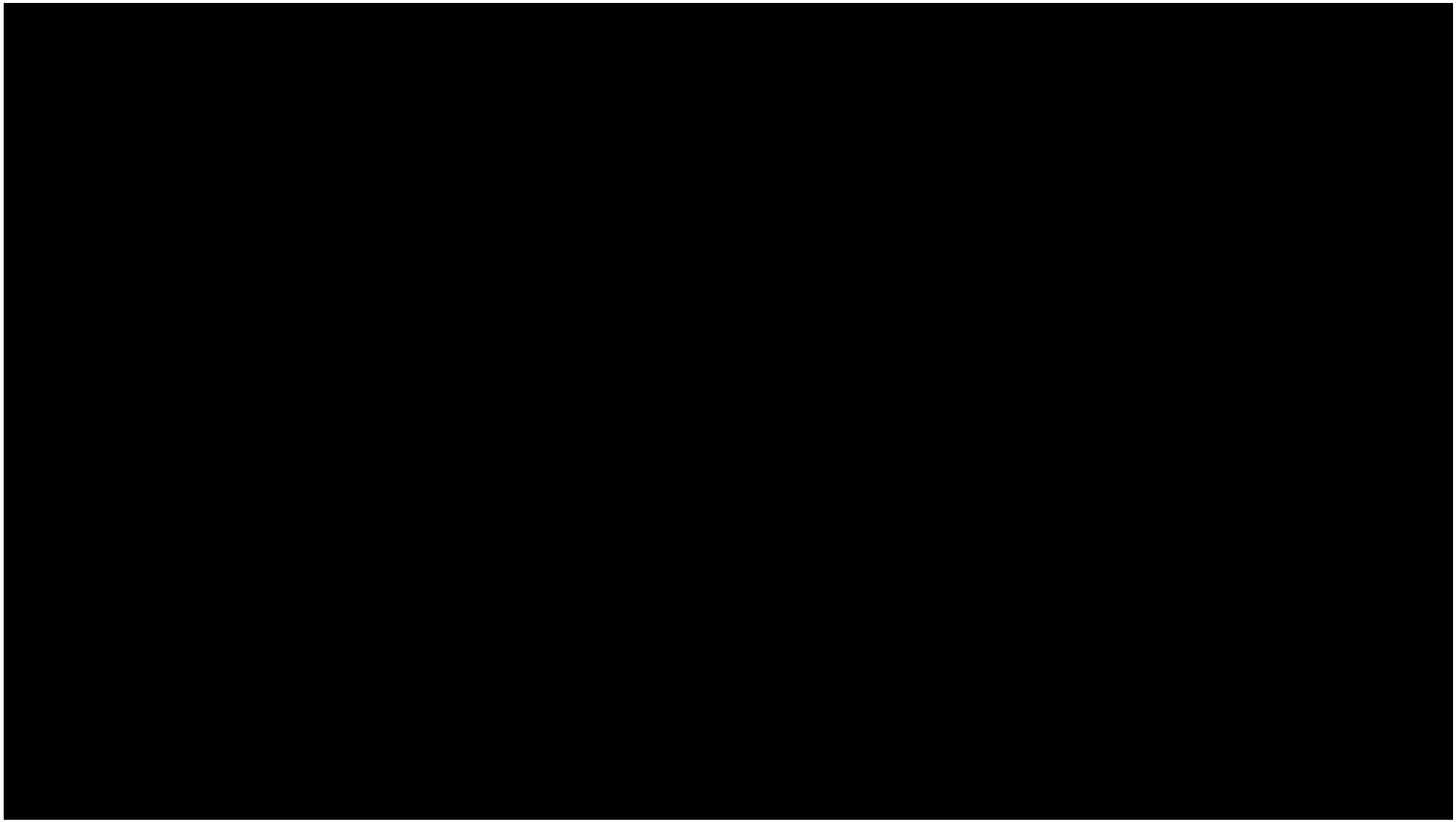
ANNEX 3 - BASELINE VOLUMES

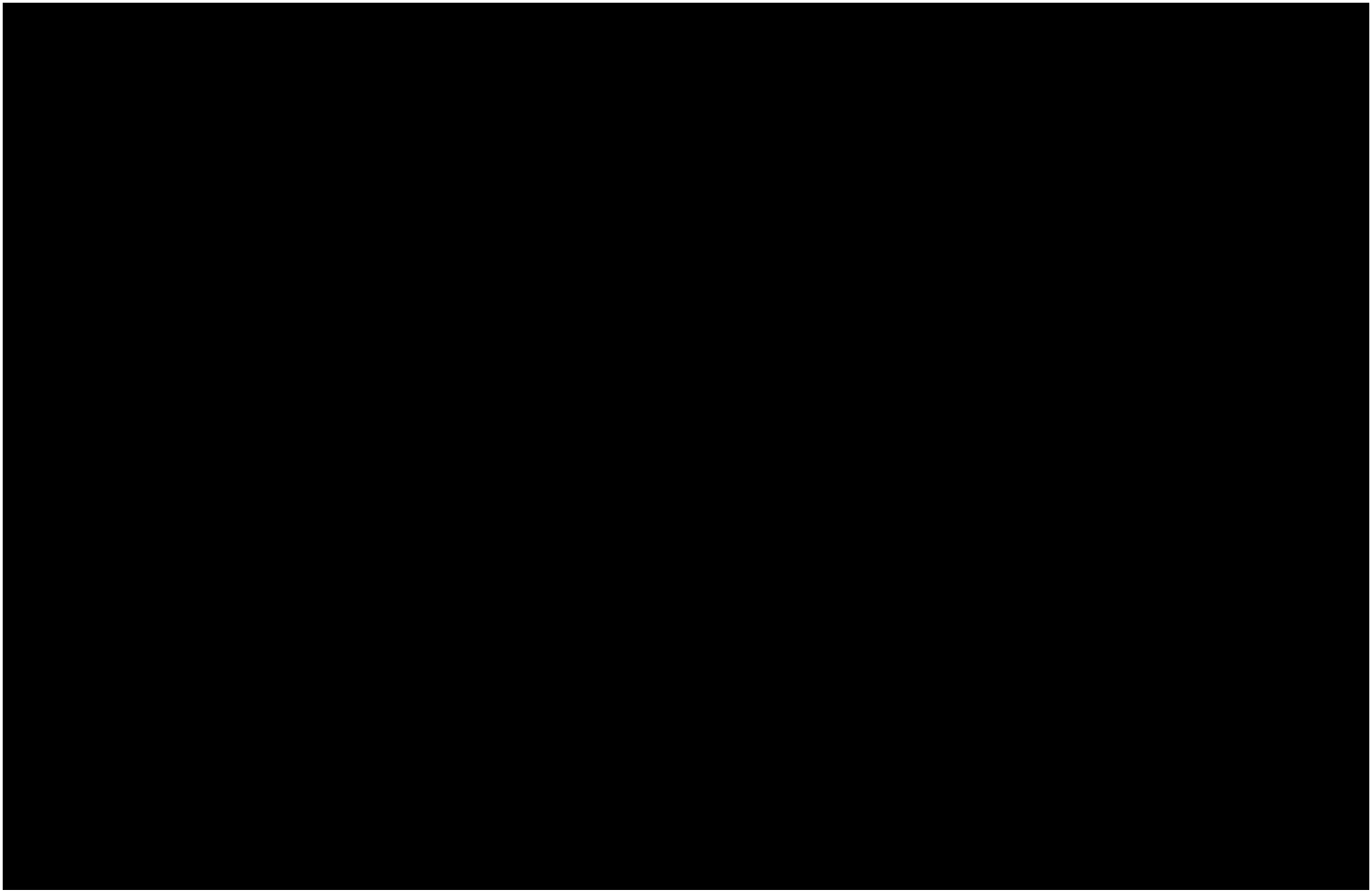


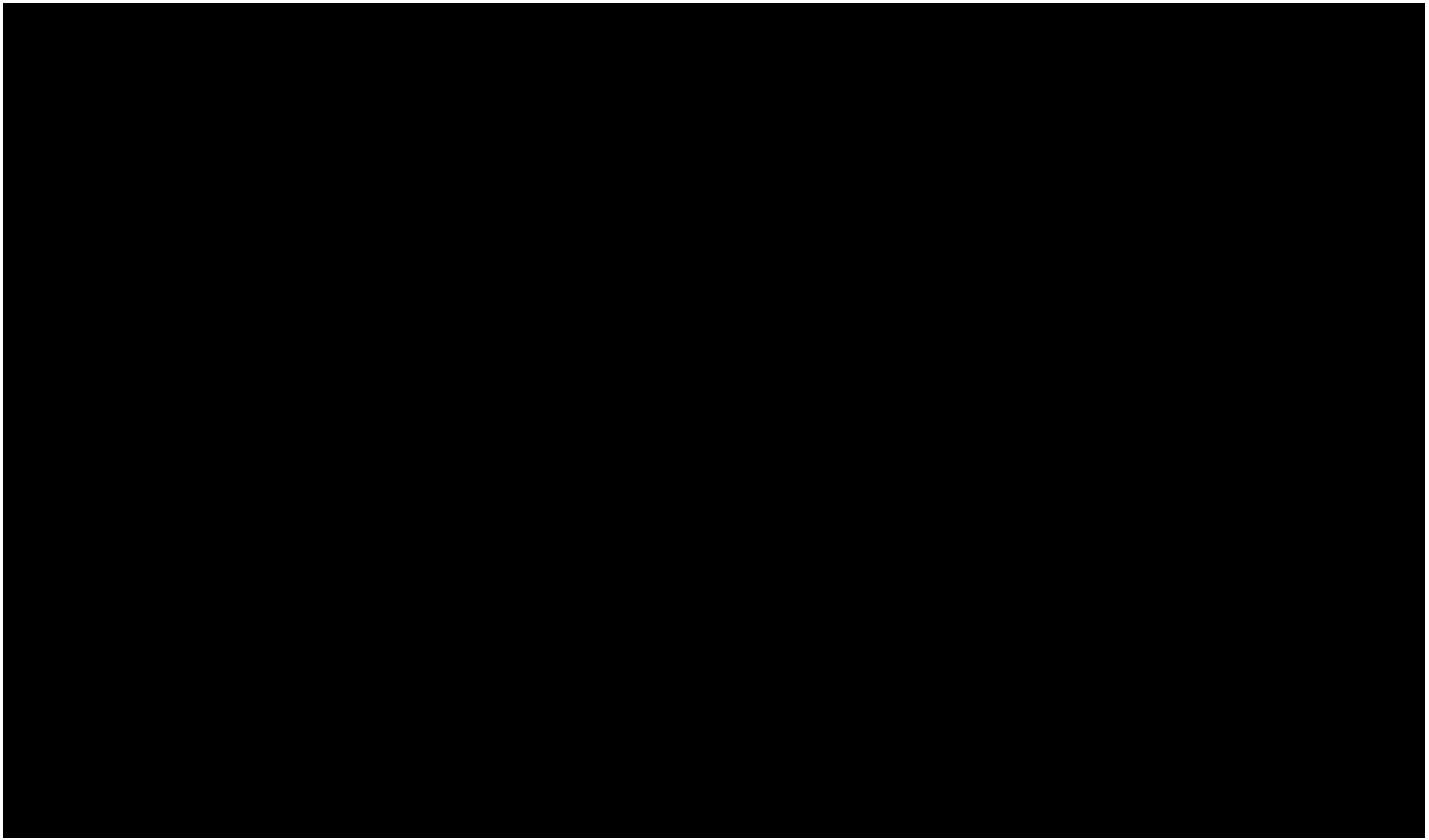
Baseline Volumes – Year 1











SCHEDULE 7.2 - PAYMENTS ON TERMINATION

1 DEFINITIONS

1.1 In this Schedule, the following definitions shall apply:

Applicable Supplier Personnel means any Supplier Personnel who:

(a) at the Termination Date:

(i) are employees of the Supplier;

(ii) are Dedicated Supplier Personnel;

(iii) have not transferred (and are not in scope to transfer at a later date) to the Director or the Replacement Supplier by virtue of the Employment Regulations; and

(b) are dismissed or given notice of dismissal by the Supplier within:

(i) forty (40) Working Days of the Termination Date; or

(ii) such longer period required by Law, their employment contract (as at the Termination Date) or an applicable collective agreement; and

(c) have not resigned or given notice of resignation prior to the date of their dismissal by the Supplier; and

(d) the Supplier can demonstrate to the satisfaction of the Director:

(i) are surplus to the Supplier's requirements after the Termination Date notwithstanding its obligation to provide services to its other customers;

(ii) are genuinely being dismissed for reasons of redundancy; and

(iii) have been selected for redundancy by the Supplier on objective grounds other than the fact that the Supplier is entitled to reimbursement under this provision in respect of such employees.

Breakage Costs Payment means an amount equal to the Redundancy Costs and the Contract Breakage Costs as at the Termination Date as determined in accordance with Paragraph 3.

Compensation Payment means the payment calculated in accordance with Paragraph 5.

Contract Breakage Costs means the amounts payable by the Supplier to its Key Sub-contractors or other third parties (as applicable) for terminating all relevant Key Sub-contracts or Third Party Contracts as a direct result of the early termination of this Agreement.

Dedicated Supplier Personnel means all Supplier Personnel then assigned to the Services or any part of the Services. If the Supplier is unsure as to whether Supplier Personnel are or should be regarded as so assigned, it shall consult with the Director whose view shall be determinative provided that the employee has been materially involved in the provision of the Services or any part of the Services.

Redundancy Costs means the total sum of any of the following sums paid to Applicable Supplier Personnel, each amount apportioned between the Supplier and the Director based on the time spent by such employee on the Services as a proportion of the total Service duration:

(a) any statutory redundancy payment; and

(b) in respect of an employee who was a Transferring Former Supplier Employee or a Transferring Director Employee, any contractual redundancy payment (or where such a contractual benefit on redundancy is a benefit payable from a pension scheme, the increase in cost to the Supplier as a net present value compared to the benefit payable on termination of employment without redundancy), provided that such employee was entitled to such contractual redundancy payment immediately prior to his or her transfer to the Supplier under the Employment Regulations.

Request for Estimate means a written request sent by the Director to the Supplier, requiring that the Supplier provide it with an accurate estimate of the Termination Payment and Compensation Payment that would be payable if the Director exercised its right under Clause 35.1.1 (*Termination by the Director*) to terminate this Agreement for convenience on a specified Termination Date.

Termination Estimate has the meaning given in Paragraph 10.2.

Third Party Contract means a contract with a third party entered into by the Supplier exclusively for the purpose of delivering the Services, as listed in Schedule 4.4 (*Third Party Contracts*).

Total Costs Incurred means the Costs incurred by the Supplier up to the Termination Date in the performance of this Agreement and detailed in the Financial Model (but excluding Contract Breakage Costs, Redundancy Costs and any costs the Supplier would not otherwise be able to recover through the Charges) less any Deductions up to (and including) the Termination Date.

2 TERMINATION PAYMENT

2.1 The Termination Payment payable pursuant to Clause 36.3 (*Payments by the Director*) shall be an amount equal to the aggregate of the Breakage Costs Payment.

3 BREAKAGE COSTS PAYMENT

3.1 The Supplier may recover through the Breakage Costs Payment only those costs incurred by the Supplier directly as a result of the termination of this Agreement which:

3.1.1 would not have been incurred had this Agreement continued until expiry of the Initial Term, or in the event that the Term has been extended, the expiry of the Extension Period;

3.1.2 are unavoidable, proven, reasonable, and not capable of recovery;

3.1.3 are incurred under arrangements or agreements that are directly associated with this Agreement;

3.1.4 are not Contract Breakage Costs relating to contracts or Sub-contracts with Affiliates of the Supplier; and

3.1.5 relate directly to the termination of the Services.

Limitation on Breakage Costs Payment

3.2 The Breakage Costs Payment shall not exceed the lower of:

3.2.1 the relevant limit set out in Annex 1; and

3.2.2 120% of the estimate for the Breakage Costs Payment set out in any relevant Termination Estimate.

Redundancy Costs

3.3 The Director shall not be liable under this Schedule for any costs associated with Supplier Personnel (whether relating to redundancy, redeployment or otherwise) other than the Redundancy Costs.

3.4 Where the Supplier can demonstrate that a member of Supplier Personnel will be made redundant following termination of this Agreement, but redeployment of such person is possible and would offer value for money to the Director when compared with redundancy, then the Director shall pay the Supplier the actual direct costs incurred by the Supplier or its Sub-contractor arising out of the redeployment of such person (including retraining and relocation costs) subject to a maximum amount of [redacted] per relevant member of the Supplier Personnel.

Contract Breakage Costs

3.5 The Supplier shall be entitled to Contract Breakage Costs only in respect of Third Party Contracts or Sub-contracts which:

3.5.1 are not assigned or novated to a Replacement Supplier or the Director at the request of the Director in accordance with Schedule 8.5 (*Exit Management*); and

3.5.2 the Supplier can demonstrate:

(a) are surplus to the Supplier's requirements after the Termination Date, whether in relation to use internally within its business or in providing services to any of its other customers; and

(b) have been entered into by it in the ordinary course of business.

3.6 The Supplier shall seek to negotiate termination of any Third Party Contracts or Sub-contracts with the relevant third party or Sub-contractor (as the case may be) using all reasonable endeavours to minimise the cancellation or termination charges.

3.7 Except with the prior written agreement of the Director, the Director shall not be liable for any costs (including cancellation or termination charges) that the Supplier is obliged to pay in respect of:

3.7.1 the termination of any contractual arrangements for occupation of, support of and/or services provided for Supplier premises which may arise as a consequence of the termination of this Agreement; and/or

3.7.2 Assets not yet installed at the Termination Date.

4 MITIGATION OF CONTRACT BREAKAGE COSTS AND REDUNDANCY COSTS

4.1 The Supplier agrees to use all reasonable endeavours to minimise and mitigate Contract Breakage Costs and Redundancy Costs by:

4.1.1 the appropriation of Assets, employees and resources for other purposes;

4.1.2 at the Director's request, assigning any Third Party Contracts and Sub-contracts to the Director or a third party acting on behalf of the Director; and

4.1.3 in relation to Third Party Contracts and Sub-contracts that are not to be assigned to the Director or to another third party, terminating those contracts at the earliest possible date without breach or where contractually permitted.

4.2 If Assets, employees and resources can be used by the Supplier for other purposes, then there shall be an equitable reduction in the Contract Breakage Costs and Redundancy Costs payable by the Director or a third party to the Supplier. In the event of any Dispute arising over whether the Supplier can use any Assets, employees and/or resources for other purposes and/or over the amount of the relevant equitable reduction, the Dispute shall be referred to an Expert for determination in accordance with the procedure detailed in Schedule 8.3 (*Dispute Resolution Procedure*).

5 COMPENSATION PAYMENT

5.1 The Compensation Payment payable pursuant to Clause 36.3.2 (*Payments by the Director*) shall be an amount equal to the total forecast Charges over the Shortfall Period (as stated in the Financial Response Template) multiplied by the Anticipated Contract Life Profit Margin.

5.2 For the purposes of Paragraph 5.1, the "**Shortfall Period**" means:

5.2.1 where the Director terminates this Agreement pursuant to Clause 35.1.1 (*Termination by the Director*), a number of days equal to the number of days by which the notice given (or deemed given pursuant to Paragraph 2.1.4 of Part 4 of Schedule 7.1 (*Charges and Invoicing*)) falls short of twelve (12) months; or

5.2.2 where the Supplier terminates this Agreement pursuant to Clause 35.3 (*Termination by the Supplier*), a number of days equal to the number of days by which the period from (and including) the date of the non-payment by the Authority to (and including) the Termination Date falls short of twelve (12) months,

but in each case subject to the limit set out in Paragraph 5.3.

5.3 The Compensation Payment shall be no greater than the lower of:

5.3.1 the relevant limit set out in Annex 1; and

5.3.2 120% of the estimate for the Compensation Payment set out in the relevant Termination Estimate.

6 FULL AND FINAL SETTLEMENT

6.1 Any Termination Payment and/or Compensation Payment paid under this Schedule shall be in full and final settlement of any claim, demand and/or proceedings of the Supplier in relation to any termination by the Director pursuant to Clause 35.1.1 (*Termination by the Director*) or termination by the Supplier pursuant to Clause 35.3 (*Termination by the Supplier*) (as applicable), and the Supplier shall be excluded from all other rights and remedies it would otherwise have been entitled to in respect of any such termination.

7 INVOICING FOR THE PAYMENTS ON TERMINATION

7.1 All sums due under this Schedule shall be payable by the Director to the Supplier in accordance with the payment terms set out in Schedule 7.1 (*Charges and Invoicing*).

8 SET OFF

8.1 The Director shall be entitled to set off any outstanding liabilities of the Supplier against any amounts that are payable by it pursuant to this Schedule.

9 NO DOUBLE RECOVERY

9.1 If any amount payable under this Schedule (in whole or in part) relates to or arises from any Transferring Assets then, to the extent that the Director makes any payments pursuant to Schedule 8.5 (*Exit Management*) in respect of such Transferring Assets, such payments shall be deducted from the amount payable pursuant to this Schedule.

9.2 The value of the Termination Payment and/or Compensation Payment shall be reduced or extinguished to the extent that the Supplier has already received the Charges or the financial benefit of any other rights or remedy given under this Agreement so that there is no double counting in calculating the relevant payment.

9.3 Any payments that are due in respect of the Transferring Assets shall be calculated in accordance with the provisions of the Exit Plan.

10 ESTIMATE OF TERMINATION PAYMENT AND COMPENSATION PAYMENT

10.1 The Director may issue a Request for Estimate at any time during the Term provided that no more than two (2) Requests for Estimate may be issued in any six (6) month period.

10.2 The Supplier shall within twenty (20) Working Days of receiving the Request for Estimate (or such other timescale agreed between the Parties), provide an accurate written estimate of the Termination Payment and the Compensation Payment that would be payable by the Director based on a postulated Termination Date specified in the Request for Estimate (such estimate being the "**Termination Estimate**"). The Termination Estimate shall:

10.2.1 be based on the relevant amounts set out in the Financial Model;

10.2.2 include:

(a) details of the mechanism by which the Termination Payment is calculated;

(b) full particulars of the estimated Contract Breakage Costs in respect of each Sub-contract or Third Party Contract and appropriate supporting documentation; and

(c) such information as the Director may reasonably require; and

10.2.3 state the period for which that Termination Estimate remains valid, which shall be not less than twenty (20) Working Days.

10.3 The Supplier acknowledges that issue of a Request for Estimate shall not be construed in any way as to represent an intention by the Director to terminate this Agreement.

10.4 If the Director issues a Termination Notice to the Supplier within the stated period for which a Termination Estimate remains valid, the Supplier shall use the same mechanism to calculate the Termination Payment as was detailed in the Termination Estimate unless otherwise agreed in writing between the Supplier and the Director.

ANNEX 1: MAXIMUM PAYMENTS ON TERMINATION

The table below sets out, by Contract Year, the maximum amount of the Breakage Costs Payment and the Compensation Payment that the Director shall be liable to pay to the Supplier pursuant to this Agreement:

Termination Date	Maximum Breakage Costs Payment	Maximum Compensation Payment
During Implementation Period	[redacted]	[redacted]
Anytime in the first Contract Year	[redacted]	[redacted]
Anytime in the second Contract Year	[redacted]	[redacted]
Anytime in the third Contract Year	[redacted]	[redacted]
Anytime in the remaining Initial Term	[redacted]	[redacted]
During Extension Period	[redacted]	[redacted]

SCHEDULE 7.3 - BENCHMARKING

1 DEFINITIONS

1.1 In this Schedule, the following definitions shall apply:

Benchmarked Service means a Service that the Director elects to include in a Benchmark Review under Paragraph 2.1.

Benchmarker means the independent third party appointed under Paragraph 3.1.

Benchmark Report means the report produced by the Benchmarker following the Benchmark Review as further described in Paragraph 5.

Benchmark Review means a review of one or more of the Services carried out in accordance with Paragraph 4 to determine whether those Services represent Good Value.

Comparable Service in relation to a Benchmarked Service, a service that is identical or materially similar to the Benchmarked Service (including in terms of scope, specification, volume and quality of performance).

Comparison Group in relation to a Comparable Service, a sample group of organisations providing the Comparable Service identified by the Benchmarker under Paragraph 4.8 which consists of organisations which are either of similar size to the Supplier or which are similarly structured in terms of their business and their service offering so as to be (in the Benchmarker's professional opinion) fair comparators with the Supplier or which, in the professional opinion of the Benchmarker, are best practice organisations and, where there are a reasonable number of such organisations, referencing only those organisations that are carrying on at least a significant part of their business within the United Kingdom.

Equivalent Services Data in relation to a Comparable Service, data derived from an analysis of the Comparable Service provided by the Comparison Group as adjusted in accordance with Paragraphs 4.8.1 and 4.9 provided that the Benchmarker shall not use any such data that relates to a period which ended more than thirty-six (36) months prior to the date of the appointment of the Benchmarker.

Good Value in relation to a Benchmarked Service, that:

(a) having taken into account the Performance Indicators and Target Performance Levels, the value for money of the Charges attributable to that Benchmarked Service is at least as good as the value for money of the Upper Quartile; and

(b) any Performance Indicators and Target Performance Levels applicable to that Benchmarked Service are, having taken into account the Charges, equal to or better than the median service levels for the Comparable Service using Equivalent Services Data; and

Upper Quartile means the top 25% of instances of provision of a Comparable Service by members of the Comparison Group ranked by best value for money to the recipients of that Comparable Service.

2 FREQUENCY, PURPOSE AND SCOPE OF BENCHMARK REVIEW

2.1 Notwithstanding the Supplier's obligation to maintain and provide access to the Open Book Data under Schedule 7.5 (*Financial Reports, Audit and Risk*), the Director may, by written notice to the Supplier, require a Benchmark Review of any or all of the following Services (as described in Schedule 2.1 (*Services Description*)) in order to establish whether a Benchmarked Service is, and/or the Benchmarked Services as a whole are, Good Value:

2.1.1 Contact Centre;

2.1.2 back office;

2.1.3 document management;

2.1.4 mail-in scanning; and

2.1.5 print and dispatch.

2.2 The Director shall be entitled to carry out a Benchmark Review of any or all Services at intervals of not less than twelve (12) months after any previous Benchmark Review relating to the same Services.

2.3 In the event the Director wishes to exercise its right to extend the Agreement at the end of the Term, the Director shall be entitled to carry out a Benchmark Review prior to any extension decision, and the findings of the Benchmark Report may be taken into consideration and used to inform any such decision of the Director.

2.4 Subject to Paragraph 2.1, the Services that are to be the Benchmarked Services shall be identified by the Director in the notice given under Paragraph 2.1.

3 APPOINTMENT OF BENCHMARKER

3.1 The Director shall appoint as the Benchmarker to carry out the Benchmark Review either an organisation on the list of organisations set out in Annex 1 (*Approved Benchmarkers*) or such other organisation as may be agreed in writing between the Parties.

3.2 The Director shall, at the written request of the Supplier, require the Benchmarker to enter into a confidentiality agreement with the Supplier in, or substantially in, the form set out in Annex 2 (*Confidentiality Agreement*).

3.3 The costs and expenses of the Benchmarker and the Benchmark Review shall be shared equally between both Parties provided that each Party shall bear its own internal costs of the Benchmark Review. The Benchmarker shall not be compensated on a contingency fee or incentive basis.

3.4 The Director shall be entitled to pay the Benchmarker's costs and expenses in full and to recover the Supplier's share from the Supplier.

4 BENCHMARK REVIEW

4.1 The Director shall require the Benchmarker to produce, and to send to each Party for approval, a draft plan for the Benchmark Review within ten (10) Working Days after the date of the appointment of the Benchmarker, or such longer period as the Benchmarker shall reasonably request in all the circumstances. The plan must include:

4.1.1 a proposed timetable for the Benchmark Review;

4.1.2 a description of the information that the Benchmarker requires each Party to provide;

4.1.3 a description of the benchmarking methodology to be used;

4.1.4 a description that clearly illustrates that the benchmarking methodology to be used is capable of fulfilling the benchmarking objectives under Paragraph 2.1;

4.1.5 an estimate of the resources required from each Party to underpin the delivery of the plan;

4.1.6 a description of how the Benchmarker will scope and identify the Comparison Group;

4.1.7 details of any entities which the Benchmarker proposes to include within the Comparison Group; and

4.1.8 if in the Benchmarker's professional opinion there are no Comparable Services or the number of entities carrying out Comparable Services is insufficient to create a Comparison Group, a detailed approach for meeting the relevant benchmarking objective(s) under Paragraph 2.1 using a proxy for the Comparison Services and/or Comparison Group as applicable.

4.2 The Parties acknowledge that the selection and/or use of proxies for the Comparison Group (both in terms of number and identity of entities) and Comparable Services shall be a matter for the Benchmarker's professional judgment.

4.3 Each Party shall give notice in writing to the Benchmarker and to the other Party within ten (10) Working Days after receiving the draft plan either approving the draft plan or suggesting amendments to that plan, which must be reasonable. Where a Party suggests amendments to the draft plan pursuant to this Paragraph, the Benchmarker shall, if it believes the amendments are reasonable, produce an amended draft plan. Paragraph 4.1 and this Paragraph shall apply to any amended draft plan.

4.4 Failure by a Party to give notice under Paragraph 4.3 shall be treated as approval of the draft plan by that Party. If the Parties fail to approve the draft plan within thirty (30) Working Days of its first being sent to them pursuant to Paragraph 4.1 then the Benchmarker shall prescribe the plan.

4.5 Once the plan is approved by both Parties or prescribed by the Benchmarker, the Benchmarker shall carry out the Benchmark Review in accordance with the plan. Each Party shall procure that all the information described in the plan, together with any additional information reasonably required by the Benchmarker is provided to the Benchmarker without undue delay. If the Supplier fails to provide any information requested from it by the Benchmarker and described in the plan, such failure shall constitute a material Default for the purposes of Clause 29.1.3 (*Rectification Plan Process*).

4.6 Each Party shall co-operate fully with the Benchmarker, including by providing access to records, technical documentation, premises, equipment, systems and personnel at times reasonably requested by the Benchmarker, provided that the Benchmarker shall be instructed to minimise any disruption to the Services.

4.7 Either Party may provide additional material to the Benchmarker to assist the Benchmarker in conducting the Benchmark Review.

4.8 Once it has received the information it requires, the Benchmarker shall:

4.8.1 finalise the sample of entities constituting the Comparison Group and collect data relating to Comparable Services. The final selection of the Comparison Group (both in terms of number and identity of entities) and of the Comparable Services shall be a matter for the Benchmarker's professional judgment;

4.8.2 derive the Equivalent Services Data by applying the adjustment factors listed in Paragraph 4.9 and from an analysis of the Comparable Services;

4.8.3 derive the relative value for money of the charges payable for the Comparable Services using the Equivalent Services Data and from that derive the Upper Quartile;

4.8.4 derive the median service levels relating to the Comparable Services using the Equivalent Services Data;

4.8.5 compare the value for money of the Charges attributable to the Benchmarked Services (having regard in particular to the applicable Performance Indicators and Target Performance Levels) to the value for money of the Upper Quartile;

4.8.6 compare the Performance Indicators and Target Performance Levels attributable to the Benchmarked Services (having regard to the Charges and Service Credits) with the median service levels using the Equivalent Services Data; and

4.8.7 determine whether or not each Benchmarked Service is and/or the Benchmarked Services as a whole are, Good Value.

4.9 The Benchmarker shall have regard to the following matters when performing a comparative assessment of a Benchmarked Service and a Comparable Service in order to derive Equivalent Services Data:

4.9.1 the contractual and business environment under which the Services are being provided (including the scope, scale, complexity and geographical spread of the Services);

4.9.2 any front-end investment and development costs of the Supplier;

4.9.3 the Supplier's risk profile including the financial, performance or liability risks associated with the provision of the Services as a whole;

4.9.4 the extent of the Supplier's management and contract governance responsibilities;

4.9.5 any other reasonable factors demonstrated by the Supplier, which, if not taken into consideration, could unfairly cause the Supplier's pricing to appear non-competitive (such as erroneous costing, non-sustainable behaviour including excessive consumption of energy or over-aggressive pricing).

5 BENCHMARK REPORT

5.1 The Benchmarker shall be required to prepare a Benchmark Report and deliver it simultaneously to both Parties, at the time specified in the plan approved under Paragraph 4, setting out its findings. The Benchmark Report shall:

5.1.1 include a finding as to whether or not each Benchmarked Service is and/or whether the Benchmarked Services as a whole are, Good Value;

5.1.2 include other findings (if any) regarding the quality and competitiveness or otherwise of those Services;

5.1.3 if any Benchmarked Service is not Good Value, or the Benchmarked Services as a whole are not Good Value, specify the changes that would be required to the Charges, Performance Indicators and/or Target Performance Levels, that would be required to make that Benchmarked Service or those Benchmarked Services as a whole Good Value; and

5.1.4 illustrate the method used for any normalisation of the Equivalent Services Data.

5.2 The Benchmarker shall act as an expert and not as an arbitrator.

5.3 If the Benchmark Report states that any Benchmarked Service is not Good Value or that the Benchmarked Services as a whole are not Good Value, then the Supplier shall (subject to Paragraphs 5.5 and 5.6) implement the changes set out in the Benchmark Report as soon as reasonably practicable within timescales agreed with the Director but in any event within no more than three (3) months. Any associated changes to the Charges shall take effect only from the same date and shall not be retrospective.

5.4 The Supplier acknowledges and agrees that Benchmark Reviews shall not result in any increase to the Charges, disapplication of the Performance Indicators or any reduction in the Target Performance Levels.

5.5 The Supplier shall be entitled to reject any Benchmark Report if the Supplier reasonably considers that the Benchmarker has not followed the procedure for the related Benchmark Review as set out in this Schedule in any material respect.

5.6 The Supplier shall not be obliged to implement any Benchmark Report to the extent this would cause the Supplier to provide the Services at a loss (as determined, by reference to the Financial Model), or to the extent the Supplier cannot technically implement the recommended changes.

5.7 In the event of any Dispute arising over whether the Benchmarker has followed the procedure for the related Benchmark Review under Paragraph 5.5 and/or any matter referred to in Paragraph 5.6, the Dispute shall be referred to Expert Determination. For the avoidance of doubt in the event of a Dispute between the Parties, the Director shall continue to pay the Charges to the Supplier in accordance with the terms of this Agreement and the Performance Indicators and Target Performance Levels shall remain unchanged pending the conclusion of the Expert Determination.

5.8 On conclusion of the Expert Determination:

5.8.1 if the Expert determines that all or any part of the Benchmark Report recommendations regarding any reduction in the Charges shall be implemented by the Supplier, the Supplier shall immediately repay to the Director the difference between the Charges paid by the Director up to and including the date of the Expert's determination and the date upon which the recommended reduction in Charges should have originally taken effect pursuant to Paragraph 5.3 together with interest thereon at the applicable rate under the Late Payment Of Commercial Debts (Interest) Act 1998; and

5.8.2 if the Expert determines that all or any part of the Benchmark Report recommendations regarding any changes to the Performance Indicators and/or Target Performance Levels shall be implemented by the Supplier:

(a) the Supplier shall immediately implement the relevant changes;

(b) the Supplier shall immediately pay an amount equal to any Service Credits which would have accrued up to and including the date of the Expert's determination if the relevant changes had taken effect on the date determined pursuant to Paragraph 5.3 together with interest thereon at the applicable rate under the Late Payment Of Commercial Debts (Interest) Act 1998; and

(c) the relevant changes shall thereafter be subject to the Change Control Procedure for the purposes of formalising and documenting the relevant change or amendment for the purposes of this Agreement.

5.9 Any failure by the Supplier to implement the changes as set out in the Benchmark Report in accordance with the relevant timescales determined in accordance with Paragraph 5.3 (unless the provisions of Paragraph 5.6 and/or Paragraph 5.7 apply) or in accordance with Paragraph 5.8 shall, without prejudice to any other rights or remedies of the Director, constitute a Supplier Termination Event.

ANNEX 1: APPROVED BENCHMARKERS

Hackett

APQC

Gartner

ISG

ANNEX 2: CONFIDENTIALITY AGREEMENT

CONFIDENTIALITY AGREEMENT

THIS AGREEMENT is made on [date]

BETWEEN:

(1) **[*insert name*]** of [***insert address***] (the "**Supplier**"); and

(2) ***[insert name]*** **of** ***[insert address]*** (the "**Benchmarker**" and together with the Supplier, the "**Parties**").

WHEREAS:

(A) The Director of Savings as agent of the Crown (the "**Director**") and the Supplier are party to a contract dated [insert date] (the "**Contract**") for the provision by the Supplier of [insert brief description of services] to the Director.

(B) The Benchmarker is to receive Confidential Information from the Supplier for the purpose of carrying out a benchmarking review for the Director of one or more of such services pursuant to the terms of the Contract (the "**Permitted Purpose**").

IT IS AGREED as follows:

1 Interpretation

1.1 In this Agreement, unless the context otherwise requires:

Confidential Information means:

(a) Information, including all personal data within the meaning of the Data Protection Act 2018, and however it is conveyed, provided by the Supplier to the Benchmarker pursuant to this Agreement that relates to:

(i) the Supplier; or

(ii) the operations, business, affairs, developments, intellectual property rights, trade secrets, know-how and/or personnel of the Supplier;

(b) other Information provided by the Supplier pursuant to this Agreement to the Benchmarker that is clearly designated as being confidential or equivalent or that ought reasonably to be considered to be confidential which comes (or has come) to the Benchmarker's attention or into the Benchmarker's possession in connection with the Permitted Purpose;

(c) discussions, negotiations, and correspondence between the Supplier or any of its directors, officers, employees, consultants or professional advisers and the Benchmarker or any of its directors, officers, employees, consultants and professional advisers in connection with the Permitted Purpose and all matters arising therefrom; and

(d) Information derived from any of the above,

but not including any Information that:

(e) was in the possession of the Benchmarker without obligation of confidentiality prior to its disclosure by the Supplier;

(f) the Benchmarker obtained on a non-confidential basis from a third party who is not, to the Benchmarker's knowledge or belief, bound by a confidentiality agreement with the Supplier or otherwise prohibited from disclosing the information to the Benchmarker;

(g) was already generally available and in the public domain at the time of disclosure otherwise than by a breach of this Agreement or breach of a duty of confidentiality; or

(h) was independently developed without access to the Confidential Information.

Information means all information of whatever nature, however conveyed and in whatever form, including in writing, orally, by demonstration, electronically and in a tangible, visual or machine-readable medium (including CD-ROM, magnetic and digital form).

Permitted Purpose has the meaning given to that expression in recital (B) to this Agreement.

1.2 In this Agreement:

1.2.1 a reference to any gender includes a reference to other genders;

1.2.2 the singular includes the plural and vice versa;

1.2.3 the words "include" and cognate expressions shall be construed as if they were immediately followed by the words "without limitation";

1.2.4 references to any statutory provision include a reference to that provision as modified, replaced, amended and/or re-enacted from time to time (before or after the date of this Agreement) and any prior or subsequent subordinate legislation made under it;

1.2.5 headings are included for ease of reference only and shall not affect the interpretation or construction of this Agreement; and

1.2.6 references to Clauses are to Clauses of this Agreement.

2 Confidentiality Obligations

2.1 In consideration of the Supplier providing Confidential Information to the Benchmarker, the Benchmarker shall:

2.1.1 treat all Confidential Information as secret and confidential;

2.1.2 have in place and maintain proper security measures and procedures to protect the confidentiality of the Confidential Information (having regard to its form and nature);

2.1.3 not disclose or permit the disclosure of any of the Confidential Information to any other person without obtaining the prior written consent of the Supplier or, if relevant, other owner or except as expressly set out in this Agreement;

2.1.4 not transfer any of the Confidential Information outside the United Kingdom;

2.1.5 not use or exploit any of the Confidential Information for any purpose whatsoever other than the Permitted Purpose;

2.1.6 immediately notify the Supplier in writing if it suspects or becomes aware of any unauthorised access, copying, use or disclosure in any form of any of the Confidential Information; and

2.1.7 once the Permitted Purpose has been fulfilled:

(a) destroy or return to the Supplier all documents and other tangible materials that contain any of the Confidential Information;

(b) ensure, so far as reasonably practicable, that all Confidential Information held in electronic, digital or other machine-readable form ceases to be readily accessible (other than by the information technology staff of the Benchmarker) from any computer, word processor, voicemail system or any other device; and

(c) make no further use of any Confidential Information.

3 Permitted Disclosures

3.1 The Benchmarker may disclose Confidential Information to those of its directors, officers, employees, consultants and professional advisers who:

3.1.1 reasonably need to receive the Confidential Information in connection with the Permitted Purpose; and

3.1.2 have been informed by the Benchmarker of the confidential nature of the Confidential Information; and

3.1.3 have agreed to terms similar to those in this Agreement.

3.2 The Benchmarker shall be entitled to disclose Confidential Information to the Director for the Permitted Purpose and to any Expert appointed in relation to a Dispute as referred to in Paragraph 5.7 of Schedule 7.3 (*Benchmarking*) to the Contract.

3.3 The Benchmarker shall be entitled to disclose Confidential Information to the extent that it is required to do so by applicable law or by order of a court or other public body that has jurisdiction over the Benchmarker.

3.4 Before making a disclosure pursuant to Clause 3.3, the Benchmarker shall, if the circumstances permit:

3.4.1 notify the Supplier in writing of the proposed disclosure as soon as possible (and if possible before the court or other public body orders the disclosure of the Confidential Information); and

3.4.2 ask the court or other public body to treat the Confidential Information as confidential.

4 General

4.1 The Benchmarker acknowledges and agrees that all property, including intellectual property rights, in Confidential Information disclosed to it by the Supplier shall remain with and be vested in the Supplier.

4.2 This Agreement does not include, expressly or by implication, any representations, warranties or other obligations:

4.2.1 to grant the Benchmarker any licence or rights other than as may be expressly stated in this Agreement;

4.2.2 to require the Supplier to disclose, continue disclosing or update any Confidential Information; or

4.2.3 as to the accuracy, efficacy, completeness, capabilities, safety or any other qualities whatsoever of any Information or materials provided pursuant to or in anticipation of this Agreement.

4.3 The rights, powers and remedies provided in this Agreement are cumulative and not exclusive of any rights, powers or remedies provided by law. No failure or delay by either Party to exercise any right, power or remedy will operate as a waiver of it nor will any partial exercise preclude any further exercise of the same, or of some other right, power or remedy.

4.4 Without prejudice to any other rights or remedies that the Supplier may have, the Benchmarker acknowledges and agrees that damages alone may not be an adequate remedy for any breach by the Benchmarker of any of the provisions of this Agreement. Accordingly, the Benchmarker acknowledges that the Supplier shall be entitled to the remedies of injunction and specific performance as well as any other equitable relief for any threatened or actual breach of this Agreement and/or breach of confidence and that no proof of special damages shall be necessary for the enforcement of such remedies.

4.5 The maximum liability of the Benchmarker to the Supplier for any breach of this Agreement shall be limited to ten million pounds (£10,000,000).

4.6 For the purposes of the Contracts (Rights of Third Parties) Act 1999 no one other than the Parties has the right to enforce the terms of this Agreement.

4.7 Each Party shall be responsible for all costs incurred by it or on its behalf in connection with this Agreement.

4.8 This Agreement may be executed in any number of counterparts and by the Parties on separate counterparts, but shall not be effective until each Party has executed at least one counterpart. Each counterpart shall constitute an original of this Agreement, but all the counterparts shall together constitute but one and the same instrument.

5 Notices

5.1 Any notice to be given under this Agreement (each a "**Notice**") shall be given in writing and shall be delivered by hand and shall be deemed to have been duly given at the time of delivery provided that such Notice is sent to the relevant physical address, and expressly marked for the attention of the relevant individual, set out in Clause 5.2.

5.2 Any Notice:

5.2.1 if to be given to the Supplier shall be sent to:

[*Address*]

Attention: [*Contact name and/or position, e.g. "The Finance Director"*]

5.2.2 if to be given to the Benchmarker shall be sent to:

[*Name of Organisation*]

[*Address*]

Attention: [ ]

6 Governing law

6.1 This Agreement shall be governed by, and construed in accordance with, English law and any matter claim or dispute arising out of or in connection with this Agreement whether contractual or non-contractual, shall be governed by and determined in accordance with English law.

6.2 Each Party hereby irrevocably submits to the exclusive jurisdiction of the English courts in respect of any claim or dispute arising out of or in connection with this Agreement.

IN WITNESS of the above this Agreement has been signed by the duly authorised representatives of the Parties on the date which appears at the head of the first page.

For and on behalf of [*name of Supplier*]

Signature: _____ Date:

Name: Position:

For and on behalf of [name of Benchmarker]

Signature: _____ Date:

Name: Position:

SCHEDULE 7.4 - FINANCIAL DISTRESS

1 DEFINITIONS

1.1 In this Schedule, the following definitions shall apply:

Applicable Financial Indicators means the financial indicators from Paragraph 5.1 of this Schedule which are to apply to the Monitored Suppliers as set out in Paragraph 5.2 of this Schedule.

Board means the Supplier's board of directors.

Board Confirmation means written confirmation from the Board in accordance with Paragraph 8 of this Schedule.

Credit Rating Threshold means the minimum threshold or failure score for each entity in the FDE Group as set out in Annex 2 of this Schedule;

FDE Group means the Supplier, Key Sub-contractors, the Guarantor and the Monitored Suppliers.

Financial Indicators in respect of the Supplier, Key Sub-contractors and the Guarantor, means each of the financial indicators set out at Paragraph 5.1 of this Schedule; and in respect of each Monitored Supplier, means those Applicable Financial Indicators.

Financial Target Thresholds means the target thresholds for each of the Financial Indicators set out at Paragraph 5.1 of this Schedule.

Monitored Suppliers means those entities specified at Paragraph 5.2 of this Schedule.

Rating Agencies means the rating agencies listed in Annex 1 of this Schedule.

2 WARRANTIES AND DUTY TO NOTIFY

2.1 The Supplier warrants and represents to the Director for the benefit of the Director that as at the Effective Date:

2.1.1 the long term credit ratings issued for each entity in the FDE Group by each of the Rating Agencies are as set out in Annex 2 of this Schedule; and

2.1.2 (subject to Paragraph 2.6) the financial position or, as appropriate, the financial performance of each of the Supplier, Guarantor and Key Sub-contractors satisfies the Financial Target Thresholds.

2.2 The Supplier shall promptly notify (or shall procure that its auditors promptly notify) the Director in writing if there is any downgrade in the credit rating issued by any Rating Agency for any entity in the FDE Group (and in any event within five (5) Working Days of the occurrence of the downgrade).

2.3 The Supplier shall:

2.3.1 regularly monitor the credit ratings of each entity in the FDE Group with the Rating Agencies;

2.3.2 monitor and report on the Financial Indicators for each entity in the FDE Group against the Financial Target Thresholds at least at the frequency set out for each at Paragraph 5.1 (where specified) and in any event, on a regular basis and no less than once a year within one hundred and twenty (120) days after the Accounting Reference Date; and

2.3.3 promptly notify (or shall procure that its auditors promptly notify) the Director in writing following the occurrence of a Financial Distress Event or any fact, circumstance or matter

which could cause a Financial Distress Event (and in any event, ensure that such notification is made within ten (10) Working Days of the date on which the Supplier first becomes aware of the Financial Distress Event or the fact, circumstance or matter which could cause a Financial Distress Event).

2.4 For the purposes of determining whether a Financial Distress Event has occurred pursuant to the provisions of Paragraph 3.1.1, and for the purposes of determining relief under Paragraph 7.1, the credit rating of an FDE Group entity shall be deemed to have dropped below the applicable Credit Rating Threshold if:

2.4.1 any of the Rating Agencies have given a Credit Rating Level for that entity which is below the applicable Credit Rating Threshold; or

2.4.2 a Rating Agency that is specified as holding a Credit Rating for an entity as set out at Annex 2 of this Schedule ceases to hold a Credit Rating for that entity.

2.5 Each report submitted by the Supplier pursuant to Paragraph 2.3.2 shall:

2.5.1 be a single report with separate sections for each of the FDE Group entities;

2.5.2 contain a sufficient level of information to enable the Director to verify the calculations that have been made in respect of the Financial Indicators;

2.5.3 include key financial and other supporting information (including any accounts data that has been relied on) as separate annexes;

2.5.4 be based on the audited accounts for the date or period on which the Financial Indicator is based or, where the Financial Indicator is not linked to an accounting period or an accounting reference date, on unaudited management accounts prepared in accordance with their normal timetable; and

2.5.5 include a history of the Financial Indicators reported by the Supplier in graph form to enable the Director to easily analyse and assess the trends in financial performance.

2.6 The Parties acknowledge that, as at the Effective Date, one or more entities in the FDE Group do not satisfy the Financial Target Threshold for the Financial Indicators as set out in Paragraph 5.2 ("**Financial Non Compliances**"). Subject to Paragraphs 2.2 and 2.3, the Supplier shall not be deemed to be in default under Paragraphs 2.1.2 and 3.1.7, and shall not be deemed to have suffered a Financial Distress Event as a result of the Financial Non Compliances. For the avoidance of doubt, no further Financial Indicators shall be incorporated within the definition of Financial Non Compliances following the Effective Date.

2.7 Notwithstanding Paragraph 2.1 (and in addition to its other reporting obligations set out in this Schedule), the Supplier shall:

(a) monitor the position of the FDE Group entities monthly as against the Financial Indicators comprising the Financial Non Compliances and promptly inform the Director in writing when any of the Financial Target Thresholds for the Financial Indicators contained within the Financial Non Compliances are met; and

(b) provide a written report to the Director (no later than the last day of each month of the Term) setting out the current position as against the Financial Target Thresholds for each of the Financial Indicators comprising the Financial Non Compliances.

2.8 When an FDE Group entity meets any of the Financial Target Thresholds for the Financial Indicators contained within the Financial Non Compliances then (i) such Financial Indicator(s) shall no longer be deemed to be included within the definition of "Financial Non Compliances", (ii) Paragraphs 2.6 and 2.7 shall no longer apply to such Financial Indicator(s), (iii) the Supplier shall be deemed to give the warranty in relation to Financial Threshold Targets for such Financial Indicator(s) as set out in Paragraph 2.1.2 as at the date the relevant Financial Target Threshold(s) are met and, (iv) this

Schedule shall apply in full to such Financial Indicators from the date the relevant Financial Target Threshold(s) are met.

3 FINANCIAL DISTRESS EVENTS

3.1 The following shall be Financial Distress Events:

3.1.1 the credit rating of an FDE Group entity dropping below the applicable Credit Rating Threshold;

3.1.2 an FDE Group entity issuing a profits warning to a stock exchange or making any other public announcement, in each case about a material deterioration in its financial position or prospects;

3.1.3 there being a public investigation into improper financial accounting and reporting, suspected fraud or any other impropriety of an FDE Group entity;

3.1.4 an FDE Group entity committing a material breach of covenant to its lenders;

3.1.5 a Key Sub-contractor notifying the Director that the Supplier is two (2) or more months in arrears of all sums properly due under the relevant Sub-contract and not subject to a genuine dispute;

3.1.6 any of the following:

(a) commencement of any litigation against an FDE Group entity with respect to financial indebtedness greater than [redacted] ([redacted]) or obligations under a service contract with a total contract value greater than [redacted] ([redacted]);

(b) non-payment by an FDE Group entity of any financial indebtedness;

(c) any financial indebtedness of an FDE Group entity becoming due as a result of an event of default;

(d) the cancellation or suspension of any financial indebtedness in respect of an FDE Group entity; or

(e) the external auditor of an FDE Group entity expressing a qualified opinion on, or including an emphasis of matter in, its opinion on the statutory accounts of that FDE entity,

in each case which the Director reasonably believes (or would be likely to reasonably believe) could directly impact on the continued performance and delivery of the Services in accordance with this Agreement; and

3.1.7 any one or more of the Financial Indicators set out at Paragraph 5 for any of the FDE Group entities failing to meet the required Financial Target Threshold.

4 CONSEQUENCES OF FINANCIAL DISTRESS EVENTS

4.1 Immediately upon notification by the Supplier of a Financial Distress Event (or if the Director becomes aware of a Financial Distress Event without notification and brings the event to the attention of the Supplier), the Supplier shall have the obligations and the Director shall have the rights and remedies as set out in Paragraphs 4.3 to 4.6.

4.2 In the event of a late or non-payment of a Key Sub-contractor pursuant to Paragraph 3.1.5, the Director shall not exercise any of its rights or remedies under Paragraph 4.3 without first giving the Supplier ten (10) Working Days to:

4.2.1 rectify such late or non-payment; or

4.2.2 demonstrate to the Director's reasonable satisfaction that there is a valid reason for late or non-payment.

4.3 The Supplier shall (and shall procure that any Monitored Supplier, the Guarantor and/or any relevant Key Sub-contractor shall):

4.3.1 at the request of the Director, meet the Director as soon as reasonably practicable (and in any event within three (3) Working Days of the initial notification (or awareness) of the Financial Distress Event or such other period as the Director may permit and notify to the Supplier in writing) to review the effect of the Financial Distress Event on the continued performance and delivery of the Services in accordance with this Agreement; and

4.3.2 where the Director reasonably believes (taking into account the discussions and any representations made under Paragraph 4.3.1) that the Financial Distress Event could impact on the continued performance and delivery of the Services in accordance with this Agreement:

(a) submit to the Director for its approval, a draft Financial Distress Remediation Plan as soon as reasonably practicable (and in any event, within ten (10) Working Days of the initial notification (or awareness) of the Financial Distress Event or such other period as the Director may permit and notify to the Supplier in writing); and

(b) to the extent that it is legally permitted to do so and subject to Paragraph 4.8, provide such information relating to the Supplier, any Monitored Supplier, Key Sub-contractors and/or the Guarantor as the Director may reasonably require in order to understand the risk to the Services, which may include forecasts in relation to cash flow, orders and profits and details of financial measures being considered to mitigate the impact of the Financial Distress Event.

4.4 The Director shall not withhold its approval of a draft Financial Distress Remediation Plan unreasonably. If the Director does not approve the draft Financial Distress Remediation Plan, it shall inform the Supplier of its reasons and the Supplier shall take those reasons into account in the preparation of a further draft Financial Distress Remediation Plan, which shall be resubmitted to the Director within five (5) Working Days of the rejection of the first draft. This process shall be repeated until the Financial Distress Remediation Plan is approved by the Director or referred to the Dispute Resolution Procedure under Paragraph 4.5.

4.5 If the Director considers that the draft Financial Distress Remediation Plan is insufficiently detailed to be properly evaluated, will take too long to complete or will not ensure the continued performance of the Supplier's obligations in accordance with the Agreement, then it may either agree a further time period for the development and agreement of the Financial Distress Remediation Plan or escalate any issues with the draft Financial Distress Remediation Plan using the Dispute Resolution Procedure.

4.6 Following approval of the Financial Distress Remediation Plan by the Director, the Supplier shall:

4.6.1 on a regular basis (which shall not be less than fortnightly):

(a) review and make any updates to the Financial Distress Remediation Plan as the Supplier may deem reasonably necessary and/or as may be reasonably requested by the Director, so that the plan remains adequate, up to date and ensures the continued performance and delivery of the Services in accordance with this Agreement; and

(b) provide a written report to the Director setting out its progress against the Financial Distress Remediation Plan, the reasons for any changes made to the Financial Distress Remediation Plan by the Supplier and/or the reasons why the Supplier may have decided not to make any changes;

4.6.2 where updates are made to the Financial Distress Remediation Plan in accordance with Paragraph 4.6.1, submit an updated Financial Distress Remediation Plan to the Director for its approval, and the provisions of Paragraphs 4.4 and 4.5 shall apply to the review and approval process for the updated Financial Distress Remediation Plan; and

4.6.3 comply with the Financial Distress Remediation Plan (including any updated Financial Distress Remediation Plan) and ensure that it achieves the financial and performance requirements set out in the Financial Distress Remediation Plan.

4.7 Where the Supplier reasonably believes that the relevant Financial Distress Event under Paragraph 4.1 (or the circumstance or matter which has caused or otherwise led to it) no longer exists, it shall notify the Director and the Parties may agree that the Supplier shall be relieved of its obligations under Paragraph 4.6.

4.8 The Supplier shall use reasonable endeavours to put in place the necessary measures to ensure that the information specified at Paragraph 4.3.2(b) is available when required and on request from the Director and within reasonable timescales. Such measures may include:

4.8.1 obtaining in advance written authority from Key Sub-contractors, the Guarantor and/or Monitored Suppliers authorising the disclosure of the information to the Director and/or entering into confidentiality agreements which permit disclosure;

4.8.2 agreeing in advance with the Director, Key Sub-contractors, the Guarantor and/or Monitored Suppliers a form of confidentiality agreement to be entered by the relevant parties to enable the disclosure of the information to the Director;

4.8.3 putting in place any other reasonable arrangements to enable the information to be lawfully disclosed to the Director (which may include making price sensitive information available to Director nominated personnel through confidential arrangements, subject to their consent); and

4.8.4 disclosing the information to the fullest extent that it is lawfully entitled to do so, including through the use of redaction, anonymisation and any other techniques to permit disclosure of the information without breaching a duty of confidentiality.

5 FINANCIAL INDICATORS

5.1 Subject to the calculation methodology and guidance set out in the Assessing and Monitoring the Economic and Financial Standing of Suppliers Guidance Note May 2021 (Assessing and Monitoring Suppliers EFS May 2021) and the provisions of Paragraphs 2.6 to 2.8, the Financial Indicators and the corresponding calculations and thresholds used to determine whether a Financial Distress Event has occurred in respect of those Financial Indicators, shall be as follows:

Financial Indicator	Description	Calculation	Financial Target Threshold	Monitoring and Reporting Frequency
Turnover Ratio	The total turnover of the Supplier (or, where the SQ is being submitted on behalf of a consortium, the total turnover of the consortium members).	Turnover Ratio = Supplier Annual Revenue / Expected Annual Contract Value	Above 2.0 for each of the last two years	Tested and reported yearly in arrears within 90 days of each accounting reference date
Operating Margin	Measures what proportion of revenues remain after deducting operating expenses.	Operating Margin = (Operating profit + Exceptional and non-underlying	Above 10.0% for each of	Tested and reported yearly in arrears within 90 days of each

Financial Indicator	Description	Calculation	Financial Target Threshold	Monitoring and Reporting Frequency
	Operating profit is calculated as the sum of: Other operating income/expense, Administrative income/expense, Grant income (e.g. Government income), Impairment losses/gains and Restructuring costs.	items*) / Turnover *Exceptional and non-underlying items are only included if value is negative.	the last two years	accounting reference date
Net Debt to EBITDA Ratio	Shows how many years it would take to repay net debt if EBITDA remained constant and was used in full to repay financial debt. Where Net Debt is defined as: **The sum of** 1. Current Liabilities: Loans and overdrafts, Deferred consideration, Lease liabilities, Amounts owed to group undertakings, Amounts owed to joint ventures and associates and Derivative financial instruments. 2. Non-current liabilities: Lease liabilities, Loans and borrowings, Amounts owed to group undertakings, Amounts owed to joint ventures and associates, Deferred consideration and Derivative financial instruments. **Less** 1. Current Assets: Derivative financial instruments, Other current financial assets (i.e. MMFs, secured loan notes), Cash and cash equivalents (Inc. marketable securities) and Investments. **Where EBITDA is defined as:** Operating profit plus	Net Debt to EBITDA Ratio = Net Debt/EBIDTA	Below 3.0 for each of the last two years	Tested and reported yearly in arrears within 90 days of each accounting reference date based upon EBITDA for the 12 months ending on the relevant accounting reference date

Financial Indicator	Description	Calculation	Financial Target Threshold	Monitoring and Reporting Frequency
	Exceptional and non-underlying items* less Depreciation and Amortisation. Operating profit is calculated as the sum of: Other operating income/expense, Administrative income/expense, Grant income (e.g. Government income), Impairment losses/gains and Restructuring costs. *Exceptional and non-underlying items are included in the calculation where the value is negative.			
Net Debt and Net Pension Deficit to EBITDA Ratio	Incorporates the Supplier's net pension deficit/surplus into the Net Debt to EBITDA Ratio. Where Net Debt is defined as: **The sum of** 1. Current Liabilities: Loans and overdrafts, Deferred consideration, Lease liabilities, Amounts owed to group undertakings, Amounts owed to joint ventures and associates and Derivative financial instruments. 2. Non-current liabilities: Lease liabilities, Loans and borrowings, Amounts owed to group undertakings, Amounts owed to joint ventures and associates, Deferred consideration and Derivative financial instruments. **Less**	Net Debt and Net Pension Deficit to EBITDA Ratio = (Net debt + Net Pension Deficit) / EBITDA	Below 4.5 for each of the last two years	Tested and reported yearly in arrears within 90 days of each accounting reference date based upon EBITDA for the 12 months ending on, and the Net Debt and Net Pension Deficit at, the relevant accounting reference date

Financial Indicator	Description	Calculation	Financial Target Threshold	Monitoring and Reporting Frequency
	1. Current Assets: Derivative financial instruments, Other current financial assets (i.e. MMFs, secured loan notes), Cash and cash equivalents (Inc. marketable securities) and Investments. **Where Net Pension Deficit is defined as:** - (Employee benefit assets (Pension etc.) - Employee benefit liabilities (Pension etc.)) **Where EBITDA is defined as:** Operating profit plus Exceptional and non-underlying items* less Depreciation and Amortisation. Operating profit is calculated as the sum of: Other operating income/expense, Administrative income/expense, Grant income (e.g. Government income), Impairment losses/gains and Restructuring costs. *Exceptional and non-underlying items are included in the calculation where the value is negative.			
Net Interest Paid Cover	A measure of how many times an organisation can cover its annual interest payments out of its available earnings.	Net Interest Paid Cover = (Operating profit + Exceptional and non-underlying items* + Share of results of associates and joint ventures) / - (Interest Received + Interest Paid) *Exceptional and non-underlying	Above 4.5 for each of the last two years	Tested and reported yearly in arrears within 90 days of each accounting reference date

Financial Indicator	Description	Calculation	Financial Target Threshold	Monitoring and Reporting Frequency
		items are only included if value is negative. Operating profit is calculated as the sum of: Other operating income/expense, Administrative income/expense, Grant income (e.g. Government income), Impairment losses/gains and Restructuring costs.		
Acid Ratio	A liquidity ratio which measures an organisation's ability to use Cash and other assets it can quickly translate into cash to meet short-term liabilities falling due.	Acid Ratio = (Current Assets - Stock and WIP) / Current liabilities	Above 1.0 for each of the last two years	Tested and reported yearly in arrears within 90 days of each accounting reference date
Net Asset Value	The value of all of an organisations assets minus all of its liabilities.	Net Asset Value = Net Worth	Above zero for each of the last two years	Tested and reported yearly in arrears within 90 days of each accounting reference date
Group Exposure Ratio	Measures the ability of the bidder to withstand the non-recovery of balances owed to it by other members of the group and/or the crystallisation of contingent liabilities linked to the wider group. Where Group Exposure is defined as: **The sum of:** 1. Other non-current assets: Amounts owed by group undertakings and Amounts owed by joint ventures and associates. 2. Current assets: Amounts owed by group undertakings and Amounts	Group Exposure Ratio = Group Exposure / Gross Assets	Below 25% for each of the last two years	Tested and reported yearly in arrears within 90 days of each accounting reference date

Financial Indicator	Description	Calculation	Financial Target Threshold	Monitoring and Reporting Frequency
	owed by joint ventures and associates. 3. Contingent liabilities in support of group undertakings (£'000s). Where Gross Assets is defined as: **The sum of:** 1. Fixed Assets: Other intangible fixed assets, Tangible fixed assets, Other fixed assets (Fixed asset investments, investment properties etc.) and Right of use assets. 2. Current Assets. We note that Goodwill has been excluded in the calculation of gross assets.			
Trade Debtors Ratio		(Trade Debtors / Turnover) x 365	Below 60 days for each of the last two years	Tested and reported half yearly in arrears within 90 days of each half year end based upon figures at the relevant half year end
Trade Creditors Ratio	A ratio which measures the average days it is taking the company to pay its creditors. Also known as "creditor days".	(Trade Creditors / Cost of Sales) x 365	Below 60 days for each of the last two years	Tested and reported half yearly in arrears within 90 days of each half year end based upon figures at the relevant half year end

5.2 Financial Non-Compliances

FDE Group Entity	Non-compliance
Supplier	Group Exposure Ratio (83.7%)

5.3 Monitored Suppliers

Monitored Supplier	Applicable Financial Indicators (these are the Financial Indicators from the table in Paragraph 5.1 which are to apply to the Monitored Suppliers)
None at the Effective Date	

6 TERMINATION RIGHTS

6.1 Subject to Paragraphs 2.6 to 2.8, the Director shall be entitled to terminate this Agreement under Clause 35.1.3 (*Termination by the Director*) if:

6.1.1 the Supplier fails to notify the Director of a Financial Distress Event in accordance with Paragraph 2.3.3;

6.1.2 the Parties fail to agree a Financial Distress Remediation Plan (or any updated Financial Distress Remediation Plan) in accordance with Paragraphs 4.3 to 4.5; and/or

6.1.3 the Supplier fails to comply with the terms of the Financial Distress Remediation Plan (or any updated Financial Distress Remediation Plan) in accordance with Paragraph 4.6.3.

7 PRIMACY OF CREDIT RATINGS

7.1 Without prejudice to the Supplier's obligations and the Director's rights and remedies under Paragraph 2, if, following the occurrence of a Financial Distress Event pursuant to any of Paragraphs 3.1.2 to 3.1.7, the Rating Agencies review and report subsequently that the credit ratings for the FDE Group entities do not drop below the relevant Credit Rating Thresholds specified for those entities in Annex 2 of this Schedule, then:

7.1.1 the Supplier shall be relieved automatically of its obligations under Paragraphs 4.3 to 4.6; and

7.1.2 the Director shall not be entitled to require the Supplier to provide financial information in accordance with Paragraph 4.3.2(b).

8 BOARD CONFIRMATION

8.1 If this Agreement has been specified as a Critical Service Contract under Paragraph 1.1 of Part 2 (*Corporate Resolution Planning*) to Schedule 8.6 (*Service Continuity Plan and Corporate Resolution Planning*) then, subject to Paragraph 8.4 of this Schedule, the Supplier shall within one hundred and twenty (120) days after each Accounting Reference Date or within fifteen (15) months of the previous Board Confirmation (whichever is the earlier) provide a Board Confirmation to the Director in the form set out at Annex 3 of this Schedule, confirming that to the best of the Board's knowledge and belief, it is not aware of and has no knowledge:

8.1.1 that a Financial Distress Event has occurred since the later of the Effective Date or the previous Board Confirmation or is subsisting; or

8.1.2 of any matters which have occurred or are subsisting that could reasonably be expected to cause a Financial Distress Event.

8.2 The Supplier shall ensure that in its preparation of the Board Confirmation it exercises due care and diligence and has made reasonable enquiry of all relevant Supplier Personnel and other persons as is reasonably necessary to understand and confirm the position.

8.3 In respect of the first Board Confirmation to be provided under this Agreement, the Supplier shall provide the Board Confirmation within fifteen (15) months of the Effective Date if earlier than the timescale for submission set out in Paragraph 8.1 of this Schedule.

8.4 Where the Supplier is unable to provide a Board Confirmation in accordance with Paragraphs 8.1 to 8.3 of this Schedule due to the occurrence of a Financial Distress Event or knowledge of subsisting matters which could reasonably be expected to cause a Financial Distress Event, it will be sufficient for the Supplier to submit in place of the Board Confirmation, a statement from the Board of Directors to the Director (and where the Supplier is a Strategic Supplier, the Supplier shall send a copy of the statement to the Cabinet Office Markets and Suppliers Team) setting out full details of any Financial Distress Events that have occurred and/or the matters which could reasonably be expected to cause a Financial Distress Event.

ANNEX 1: RATING AGENCIES AND THEIR STANDARD RATING SYSTEM

Dun & Bradstreet

The Director shall have the right to replace Dunn & Bradstreet with an alternative Credit Referencing Agency should the Director or UK Government change its preferred Credit Rating Agency Platform.

ANNEX 2: CREDIT RATINGS AND CREDIT RATING THRESHOLDS

Entity	**Credit Rating Threshold** *(insert the actual rating (e.g AA-) or the Credit Rating Level (e.g Credit Rating Level 3)*
Supplier	Failure Score of 98 or below
Guarantor	Failure Score of 98 or below

ANNEX 3: BOARD CONFIRMATION

Supplier Name:

Contract Reference Number:

The Board of Directors acknowledge the requirements set out at Paragraph 8 of Schedule 7.4 (*Financial Distress*) and confirm that the Supplier has exercised due care and diligence and made reasonable enquiry of all relevant Supplier Personnel and other persons as is reasonably necessary to enable the Board to prepare this statement.

The Board of Directors confirms, to the best of its knowledge and belief, that as at the date of this Board Confirmation it is not aware of and has no knowledge:

(a) that a Financial Distress Event has occurred since the later of the previous Board Confirmation and the Effective Date or is subsisting; or

(b) of any matters which have occurred or are subsisting that could reasonably be expected to cause a Financial Distress Event

On behalf of the Board of Directors:

Chair ……

Signed ……

Date ……

Director ……

Signed ……

Date ……