DATED 22/11/2022

(1) NUCLEAR DECOMMISSIONING AUTHORITY

(2) RESILINC CORPORATION

NDA COMMERCIAL SYSTEMS PROCUREMENT LOT D: SUPPLY CHAIN MAPPING AND RISK MANAGEMENT SYSTEM

Relating to "Project Victory"

Ref: NDA9/00975

CONTENTS

SCHEDULES

THIS AGREEMENT is made on 22/11/2022

BETWEEN:-

(1) **NUCLEAR DECOMMISSIONING AUTHORITY** whose principal place of business is at Herdus House, Westlakes Science Park, Moor Row, Cumbria CA24 3HU (the "**Authority**"); and

(2) **RESILINC CORPORATION** a company registered in 1525 McCarthy Blvd., Suite 1122, Milpitas, CA 95035 (the "**Supplier**").

(each a "**Party**" and together the "**Parties**").

WHEREAS:-

(A) The Authority is established to deliver the decommissioning and clean-up of the UK's civil nuclear legacy and wishes to purchase corporate applications and associated services to support its internal procurement activities and those of the Service Recipients.

(B) On 26/01/2022 the Authority advertised on Find-A-Tender Service (FTS), reference 2022/S 000-002373, inviting prospective suppliers to submit proposals for the supply of the corporate applications and services as follows:

The Nuclear Decommissioning Authority (NDA) has established 'Project Victory', to replace expiring contracts and significantly enhance the NDA group's current commercial IT systems capability. The NDA group comprises Sellafield Ltd, Magnox Ltd, LLW Repository Ltd, Dounreay Site Restoration Ltd, International Nuclear Services Ltd, Direct Rail Services Ltd, and Radioactive Waste Management Ltd; and spends in the region of GBP 1.9 billion per annum with the supply chain. The new systems will cover all aspects of how we manage that spend including: our procurement pipelines, sourcing, contracts, commercial benefits and savings tracking, identifying and managing supply chain risk, and strategic supplier relationship management.

The new systems are being procured and contracted for by NDA in four parts, referred to hereafter as lots:

- Lot A: Source-to-Contract System;
- Lot B: Market Intelligence and Category Strategies;
- Lot C: Contract Management System for End-to-End Project Management Contracts;
- Lot D: Supply Chain Risk Management System.

The four parts are accompanied by an Analytics, Reporting and Dashboarding System – Lot E – a data warehouse with Microsoft Power BI that is being built by the Authority.

This Agreement is for the Lot D Supply Chain Mapping and Risk Management System. The system will

- Support identification of at least the first three tiers of our supply chain (some contracts will have deeper supply chains) for a core set of our contracts and enable the NDA group to identify, assess, mitigate and monitor risks within that scope for each category/sub-category/critical product, department and NDA group business
- Use financial and performance intelligence to identify suppliers at risk of business failure, alerting users of changes so that action can be taken
- Support the effective management of business continuity in relation to the supply chain
- Enable identification of over-reliance on single or multiple suppliers
- Enable the NDA group to map supply lines by each supplier's geographical locations and detail risk exposure to programmes and spend categories including, for example, metrics on geopolitical, macroeconomic and natural hazards
- Enable the NDA group to map where SMEs or Social Enterprises are operating in supply chains ad spend categories

- Enable the NDA group to create a live picture of the NDA group's supply chain where key Government policy agenda matters are significant, such as the potential for human rights abuse, good employment practice issues, sustainability and the environment etc to develop suitable action plans
- Enable supply chain risk mitigation within the system, including collaboration between teams

(C) The Supplier is a leading provider of Supply Chain Mapping and Risk Management Solutions and has experience in delivering Supply Chain Mapping and Risk Management Solutions and related services in a Works context.

(D) On the basis of the Supplier's response to the advertisement and a subsequent tender process, the Authority selected the Supplier as its preferred supplier.

(E) The Parties have agreed to contract with each other in accordance with the terms and conditions set out below.

IT IS AGREED as follows:-

SECTION A - PRELIMINARIES

1. **DEFINITIONS AND INTERPRETATION**

1.1 In this Agreement, unless otherwise provided or the context otherwise requires, capitalised expressions shall have the meanings set out in Schedule 1 (*Definitions*) .

1.2 In this Agreement, unless the context otherwise requires:-

1.2.1 the singular includes the plural and vice versa;

1.2.2 reference to a gender includes the other gender and the neuter;

1.2.3 references to a person include an individual, company, body corporate, corporation, unincorporated association, firm, partnership or other legal entity or Central Government Body;

1.2.4 a reference to any Law includes a reference to that Law as amended, extended, consolidated or re-enacted from time to time;

1.2.5 any reference in this Agreement which immediately before Exit Day is a reference to (as it has effect from time to time):-

(a) any EU regulation, EU decision, EU tertiary legislation or provision of the EEA agreement ("**EU References**") which is to form part of domestic law by application of section 3 of the European Union (Withdrawal) Act 2018 and which shall be read on and after Exit Day as a reference to the EU References as they form part of domestic law by virtue of section 3 of the European Union (Withdrawal) Act 2018 as modified by domestic law from time to time; and

(b) any EU institution or EU authority or other such EU body shall be read on and after Exit Day as a reference to the UK institution, authority or body to which its functions were transferred;

1.2.6 the words "**including**", "**other**", "**in particular**", "**for example**" and similar words shall not limit the generality of the preceding words and shall be construed as if they were immediately followed by the words "**without limitation**";

1.2.7 references to "**writing**" include typing, printing, lithography, photography, display on a screen, electronic and facsimile transmission and other modes of representing or reproducing words in a visible form, and expressions referring to writing shall be construed accordingly;

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

1.2.9 unless otherwise provided and save for references in Appendices 1 to 3 of Schedule 5 (*Software*), references to Clauses and Schedules are references to the Clauses and Schedules of this Agreement and references in any Schedule to paragraphs, Parts and Appendices are, unless otherwise provided, references to the paragraphs, parts and appendices of the Schedule or the Part of the Schedule in which the references appear; and

1.2.10 references to this Agreement are references to this Agreement as amended from time to time.

1.3 If there is any conflict between the Clauses and the Schedules and/or any Appendices to the Schedules, the conflict shall be resolved in accordance with the following order of precedence:-

1.3.1 the Clauses and Schedule 1 (*Definitions*);

1.3.2 Schedules 2.1 (*Services Description*) and 2.2 (*Performance Levels*) and their Appendices;

1.3.3 any other Schedules and their Appendices (other than Schedule 4.1 (*Supplier Solution*) and its Appendices); and

1.3.4 Schedule 4.1 (*Supplier Solution*) and its Appendices (if any).

1.4 The Schedules and their Appendices form part of this Agreement.

1.5 In entering into this Agreement the Authority is acting as a central purchasing body for the purposes of the Public Contracts Regulations 2015.

2. DUE DILIGENCE

2.1 The Supplier acknowledges that:-

2.1.1 the Authority has delivered or made available to the Supplier all of the information and documents that the Supplier considers necessary or relevant for the performance of its obligations under this Agreement;

2.1.2 it has made its own enquiries to satisfy itself as to the accuracy and adequacy of the Due Diligence Information;

2.1.3 it has satisfied itself (whether by inspection or having raised all relevant due diligence questions with the Authority before the Effective Date) of all relevant details relating to the Authority Requirements and the operating processes and procedures and the working methods of the Authority and the Service Recipients.

2.2 The Supplier shall not be excused from the performance of any of its obligations under this Agreement on the grounds of, nor shall the Supplier be entitled to recover any additional costs or

charges, arising as a result of any misinterpretation of the Authority Requirements and/or any failure by the Supplier to satisfy itself as to the accuracy and/or adequacy of the Due Diligence Information.

3. WARRANTIES

3.1 The Authority represents and warrants that:-

3.1.1 it has full capacity and authority to enter into and to perform this Agreement; and

3.1.2 this Agreement is executed by its duly authorised representative.

3.2 The Supplier represents and warrants that:-

3.2.1 it is validly incorporated, organised and subsisting in accordance with the Laws of its place of incorporation;

3.2.2 it has full capacity and authority to enter into and to perform this Agreement;

3.2.3 this Agreement is executed by its duly authorised representative;

3.2.4 it has all necessary consents and regulatory approvals to enter into this Agreement;

3.2.5 all written statements and representations in any written submissions made by the Supplier as part of the procurement process, including without limitation its response to the selection questionnaire, Invitation to Submit Initial Tender and any other documents submitted remain true and accurate except to the extent that such statements and representations have been superseded or varied by this Agreement or to the extent that the Supplier has otherwise disclosed to the Authority in writing prior to the date of this Agreement;

3.2.6 it has all necessary rights in and to the Licensed Software, the Third Party IPRs, the Supplier IPRs and any other materials made available by the Supplier (and/or any Sub-contractor) to the Authority which are necessary for the performance of the Supplier's obligations under this Agreement and/or the receipt of the Services by the Authority;

3.2.7 it has notified the Authority in writing of any Occasions of Tax Non-compliance- and any litigation in which it is involved that is in connection with any Occasion of Tax Non-compliance-;

3.2.8 no proceedings or other steps have been taken and not discharged (nor, to the best of its knowledge, are threatened) for the winding up of the Supplier or for its dissolution or for the appointment of a receiver, administrative receiver, liquidator, manager, administrator or similar officer in relation to any of the Supplier's assets or revenue;

3.2.9 there are currently no matters that it is aware of that could cause a Financial Distress Event to occur or subsist.

3.3 The representations and warranties set out in Clause 3.2 shall be deemed to be repeated by the Supplier on the Effective Date by reference to the facts then existing.

3.4 The fact that any provision within this Agreement is expressed as a warranty shall not preclude any right of termination which the Authority may have in respect of breach of that provision by the Supplier.

3.5 Except as expressly stated in this Agreement, all warranties and conditions whether express or implied by statute, common law or otherwise are hereby excluded to the extent permitted by Law.

SECTION B – THE SERVICES

4. TERM

4.1 This Agreement shall:-

4.1.1 come into force on the Effective Date; and

4.1.2 unless terminated at an earlier date by operation of Law or in accordance with Clause 29 (*Termination Rights*), terminate:-

(a) at the end of the Initial Term; or

(b) if the Authority elects to extend the Initial Term by giving the Supplier at least ninety (90) days' notice before the end of the Initial Term, at the end of the First Extension Period; or

(c) if the Authority elects to extend the Extended Term by giving the Supplier at least ninety (90) days' notice before the end of the First Extension Period, at the end of the Second Extension Period.

5. SERVICES

Standard of Services

5.1 The Supplier shall provide (for the benefit of the Authority and Service Recipients):-

5.1.1 the Implementation Services from (and including) the Implementation Services Commencement Date;

5.1.2 the Operational Services in each case from (and including) the relevant Operational Service Commencement Date; and

5.1.3 the Projects when commissioned by the Authority or a Service Recipient in accordance with the process set out in the Change Control Procedure.

5.2 The Supplier shall ensure that the Services:-

5.2.1 comply in all respects with the Services Description; and

5.2.2 are supplied in accordance with the Supplier Solution and the provisions of this Agreement.

5.3 The Authority may require the Supplier to provide any or all of the Services to (and for the benefit of) any or all of the Service Recipients at any time during the Term.

5.4 The Supplier shall perform its obligations under this Agreement, including in relation to the supply of the Services and any Goods in accordance with:-

5.4.1 all applicable Law;

5.4.2 Good Industry Practice;

5.4.3 the Standards;

5.4.4 the Baseline Security Requirements; and

5.4.5 the quality standard BS EN ISO 9001.

5.5 In the event that the Supplier becomes aware of any inconsistency between the requirements of Clauses 5.4.1 to 5.4.5, the Supplier shall immediately notify the Authority Representative in writing of such inconsistency and the Authority Representative shall, as soon as practicable, notify the Supplier which requirement the Supplier shall comply with.

Supplier covenants

5.6 The Supplier shall:-

5.6.1 at all times allocate sufficient resources with the appropriate technical expertise to supply the Deliverables and to provide the Services in accordance with this Agreement;

5.6.2 ensure that:-

(a) it shall continue to have all necessary rights in and to the Licensed Software, the Third Party IPRs, the Supplier IPRs and any other materials made available by the Supplier (and/or any Sub-contractor) to the Authority or any Service Recipient which are necessary for the performance of the Supplier's obligations under this Agreement and/or the receipt of the Services by the Authority and any Service Recipient;

(b) the release of any upgrade to any Software complies with the interface requirements in the Services Description or specified under the Change Control Procedure and (except in relation to new Software or upgrades which are released to address Malicious Software or to comply with the requirements of Schedule 2.4 (Security Management)); and

(c) all Software, including Upgrades, Updates and New Releases, used by or on behalf of the Supplier in providing the Services are currently supported versions of that Software and perform in all material respects in accordance with the relevant specification;

5.6.3 ensure that any Documentation and training provided by the Supplier to the Authority and all Service Recipients are comprehensive, accurate and prepared in accordance with Good Industry Practice;

5.6.4 to the extent specified in the Authority Requirements, co-operate with the Other Suppliers as specified in the Authority Requirements and provide reasonable information (including any Documentation), advice and assistance in connection with the Services to them;

5.6.5 provide the Authority and Service Recipients with such assistance as the Authority may reasonably require during the Term in respect of the supply of the Services;

5.6.6 notify the Authority in writing as soon as reasonably possible and in any event within one month of any change of Control taking place (such notification to include notification of any likely or anticipated adverse impact on the Services); and

5.6.7 notify the Authority in writing within ten (10) Working Days of their occurrence, of any actions, suits or proceedings or regulatory investigations before any court or administrative body or arbitration tribunal pending or, to its knowledge, threatened against it that might affect its ability to perform its obligations under this Agreement.

Software warranty

5.7 Without prejudice to Clauses 5.6 (*Supplier Covenants*) and any other rights and remedies of the Authority howsoever arising, the Supplier warrants to the Authority that all components of the Software shall:-

5.7.1 be free from material design and programming errors;

5.7.2 perform in all material respects in accordance with the relevant specifications contained in the Supplier Solution and Documentation; and

5.7.3 not infringe any Intellectual Property Rights.

Continuing obligation to provide the Services

5.8 The Supplier shall continue to perform all of its obligations under this Agreement and shall not suspend the supply of the Services, notwithstanding:-

5.8.1 the existence of an unresolved Dispute; and/or

5.8.2 any failure by the Authority to pay any Charges.

Authority Responsibilities

5.9 The Authority shall comply with its responsibilities set out in Schedule 3 (*Authority Responsibilities*).

6. IMPLEMENTATION

Implementation Plan and Delays

6.1 The Parties shall comply with the provisions of Schedule 6.1 (*Implementation Plan*) including in relation to the agreement and maintenance of the Detailed Implementation Plan.

6.2 The Supplier shall:-

6.2.1 comply with the Implementation Plan; and

6.2.2 ensure that each Milestone is Achieved on or before its Milestone Date.

6.3 If the Supplier becomes aware that there is, or there is reasonably likely to be, a Delay it shall:-

6.3.1 notify the Authority in accordance with Clause 26.1 (*Rectification Plan Process*);

6.3.2 comply with the Rectification Plan Process in order to address the impact of the Delay or anticipated Delay; and

6.3.3 use all reasonable endeavours to eliminate or mitigate the consequences of any Delay or anticipated Delay.

Testing and Achievement of Milestones

6.4 The Parties shall comply with the provisions of Schedule 6.2 (*Milestone Achievement Procedure*) including in relation to the procedures to determine whether a Milestone or Test has been Achieved.

7. KEY PERFORMANCE INDICATORS

7.1 The Supplier shall:-

7.1.1 provide the Operational Services in such a manner so as to meet or exceed the Target Performance Level for each Key Performance Indicator; and

7.1.2 comply with the provisions of Schedule 2.2 (*Performance Levels*) in relation to the monitoring and reporting on its performance against the Key Performance Indicators.

KPI Failures

7.2 If in any Service Period:-

7.2.1 a KPI Failure occurs, Service Credits shall be deducted from the Service Charges in accordance with paragraph 3 of Part 3 of Schedule 7.1 (*Charges and Invoicing*); and/or

7.2.2 a Material KPI Failure occurs, the Supplier shall comply with the Rectification Plan Process (in addition to Service Credits accruing in accordance with Clause 7.2.1).

7.3 Service Credits shall not be the Authority's exclusive financial remedy for a KPI Failure except where:-

7.3.1 the KPI Failure:**-**

(a) breaches the relevant KPI Service Threshold;

(b) has arisen due to the wilful default by the Supplier or any Supplier Personnel; or

(c) results in:-

(i) the corruption or loss of any Authority Data (in which case the remedies under Clause 19.7 (Authority Data and Security Requirements) shall also be available); and/or

(ii) the Authority being required to make a compensation payment to one or more third parties;

(iii) the Supplier has fraudulently misreported its performance against any Key Performance Indicator; and/or

(d) the Authority is otherwise entitled to or does terminate the relevant Services or this Agreement pursuant to Clause 29.1.2 (Termination by the Authority).

Critical Performance Failure

7.4 If a Critical Performance Failure occurs, the Authority may exercise its rights to terminate this Agreement in whole or in part pursuant to Clause 29.1 or 29.2 (*Termination by the Authority*).

8. SERVICES IMPROVEMENT

8.1 The Supplier shall have an ongoing obligation throughout the Term to identify new or potential improvements to the Services in accordance with this Clause 8. As part of this obligation the Supplier shall identify and report to the Authority both on its Product Roadmap from time to time and, in addition, once every twelve (12) months on:-

8.1.1 the emergence of new and evolving relevant technologies which could improve the IT Environment and/or the Services, and those technological advances potentially available to the Supplier and the Authority and Service Recipients which the Parties may wish to adopt;

8.1.2 new or potential improvements to the interfaces or integration of the Services with other services provided by third parties (including the Other Suppliers) or the Authority or Service Recipients which might result in efficiency or productivity gains or in reduction of operational risk; and/or

8.1.3 commercially reasonable and technically possible new or potential improvements that could by made by the other suppliers to the Authority in connection with Project Victory for the benefit of the wider programme (including those improvements that arise as a result of a Change in Law or in Good Industry Practice).

8.2 The Supplier shall ensure that the information that it provides to the Authority shall be sufficient for the Authority to decide whether any improvement should be implemented. The Supplier shall provide any further information that the Authority requests.

8.3 If the Authority wishes to incorporate any improvement identified by the Supplier the Authority shall send the Supplier a Change Request in accordance with the Change Control Procedure.

SECTION C – PAYMENT, TAXATION AND VALUE FOR MONEY PROVISIONS

9. FINANCIAL AND TAXATION MATTERS

Charges and Invoicing

9.1 In consideration of the Supplier carrying out its obligations under this Agreement, including the provision of the Services, the Authority shall pay the Charges to the Supplier in accordance with the pricing and payment profile and the invoicing procedure specified in Schedule 7.1 (*Charges and Invoicing*).

9.2 Except as otherwise provided, each Party shall each bear its own costs and expenses incurred in respect of compliance with its obligations under this Agreement including under Clauses 6.4 (*Testing and Achievement of Milestones*), 11 (*Records, Reports, Audits and Open Book Data*), 21 (*Transparency and Freedom of Information*) and 22 (*Protection of Personal Data*).

9.3 If the Authority fails to pay any undisputed Charges properly invoiced under this Agreement, the Supplier shall have the right to charge interest on the overdue amount at the applicable rate under the Late Payment of Commercial Debts (Interest) Act 1998, accruing on a daily basis from the due date up to the date of actual payment, whether before or after judgment.

VAT

9.4 The Charges are stated exclusive of VAT, which shall be added at the prevailing rate as applicable and paid by the Authority following delivery of a valid VAT invoice.

9.5 The Supplier shall indemnify the Authority on a continuing basis against any liability, including any interest, penalties or costs incurred, that is levied, demanded or assessed on the Authority at any time in respect of the Supplier's failure to account for or to pay any VAT relating to payments made to the Supplier under this Agreement. Any amounts due under this Clause 9.5 shall be paid in cleared funds by the Supplier to the Authority not less than forty five (45) Working Days before the date upon which the tax or other liability is payable by the Authority.

Set-off and Withholding

9.6 The Authority may set off any amount owed by the Supplier to the Authority against any amount due to the Supplier under this Agreement or under any other agreement between the Supplier and the Authority, provided that the Authority shall give notice to the Supplier within thirty (30) days of receipt of the relevant invoice, setting out the Authority's reasons for withholding or retaining the relevant Charges.

Financial Reporting and Financial Distress

9.7 The Supplier shall provide to the Authority:

9.7.1 Unaudited copies of financial statements once every calendar year.

9.8 If, the Authority is concerned about the Supplier’s financial condition, the Supplier shall, on the Authority’s written request, meet with the Authority within ten (10) Working Days of such request to discuss in good faith, but on a without prejudice basis, its concerns and how they might be addressed.

9.9 The rights referred to in Clause **Error! Reference source not found.** are as follows:

9.9.1 the right to require the Supplier's Chief Financial Officer (or appropriate delegate) to meet with the Authority to discuss the event and the impact on the Services and this Agreement within ten (10) Working Days of the request.

Promoting Tax Compliance

9.10 If, at any point during the Term, an Occasion of Tax Non--Compliance occurs, the Supplier shall:-

9.10.1 notify the Authority in writing of such fact within forty-five (45) Working Days of its occurrence; and

9.10.2 promptly provide to the Authority:-

(a) details of the steps which the Supplier is taking to address the Occasion of Tax Non--Compliance and to prevent the same from recurring, together with any mitigating factors that it considers relevant; and

(b) such other information in relation to the Occasion of Tax Non--Compliance as the Authority may reasonably require.

SECTION D - CONTRACT GOVERNANCE

10. **GOVERNANCE**

10.1 The Parties shall comply with the provisions of Schedule 8.1 (*Governance*) in relation to the management and governance of this Agreement.

Representatives

10.2 Each Party shall have a representative for the duration of this Agreement who shall have the authority to act on behalf of their respective Party on the matters set out in, or in connection with, this Agreement.

11. **RECORDS, REPORTS, AUDITS & OPEN BOOK DATA**

11.1 The Supplier shall comply with the provisions of:-

11.1.1 Schedule 8.4 (*Reports and Records Provisions*) in relation to the maintenance and retention of Records; and

11.1.2 Part 1 of Schedule 7.5 (*Financial Reports and Audit Rights*) in relation to the maintenance of Open Book Data.

11.2 The Parties shall comply with the provisions of:-

11.2.1 Part 2 of Schedule 7.5 (*Financial Reports and Audit Rights*) in relation to the provision of the Financial Reports; and

11.2.2 Part 3 of Schedule 7.5 (*Financial Report and Audit Rights*) in relation to the exercise of the Audit Rights by the Authority or any Audit Agents

12. CHANGE

Change Control Procedure

12.1 Any requirement for a Change shall be subject to the Change Control Procedure.

Change in Law

12.2 The Supplier shall neither be relieved of its obligations to supply the Services in accordance with the terms and conditions of this Agreement nor be entitled to an increase in the Charges as the result of:-

12.2.1 a General Change in Law; or

12.2.2 a Specific Change in Law where the effect of that Specific Change in Law on the Services is reasonably foreseeable at the Effective Date.

12.3 If a Specific Change in Law occurs or will occur during the Term (other than as referred to in Clause 12.2.2), the Supplier shall:-

12.3.1 notify the Authority as soon as reasonably practicable of the likely effects of that change, including:-

(a) whether any Change is required to the Services, the Charges or this Agreement; and

(b) whether any relief from compliance with the Supplier's obligations is required, including any obligation to Achieve a Milestone and/or to meet the Target Performance Levels; and

12.3.2 provide the Authority with evidence:-

(a) that the Supplier has minimised any increase in costs or maximised any reduction in costs, including in respect of the costs of its Sub-contractors;

(b) as to how the Specific Change in Law has affected the cost of providing the Services; and

(c) demonstrating that any expenditure that has been avoided, for example which would have been required under the provisions of Clause 8 (Services Improvement), has been taken into account in amending the Charges.

12.4 Any variation in the Charges or relief from the Supplier's obligations resulting from a Specific Change in Law (other than as referred to in Clause 12.2.2) shall be implemented in accordance with the Change Control Procedure.

SECTION E – SUPPLIER PERSONNEL AND SUPPLY CHAIN

13. SUPPLIER PERSONNEL

13.1 The Supplier shall:-

13.1.1 provide in advance of any admission to Authority Premises a list of the names of all Supplier Personnel requiring such admission, specifying the capacity in which they require admission and giving such other particulars as the Authority may reasonably require;

13.1.2 ensure that all Supplier Personnel:-

(a) are appropriately qualified, trained and experienced to provide the Services with all reasonable skill, care and diligence;

(b) are vetted in accordance with Good Industry Practice and, where applicable, the security requirements set out in Schedule 2.1 (*Services Description*); and

(c) comply with all reasonable requirements of the Authority concerning conduct at the Authority Premises, including the security requirements as set out in Schedule 2.4 (*Security Management*);

13.1.3 subject to Schedule 9.1 (*Staff Transfer*), retain overall control of the Supplier Personnel at all times so that the Supplier Personnel shall not be deemed to be employees, agents or contractors of the Authority; and

13.1.4 be liable at all times for all acts or omissions of Supplier Personnel, so that any act or omission of a member of any Supplier Personnel which results in a Default under this Agreement shall be a Default by the Supplier.

13.2 If the Authority reasonably believes that any of the Supplier Personnel are unsuitable to undertake work in respect of this Agreement, it may:-

13.2.1 refuse admission to the relevant person(s) to the Authority Premises; and/or

13.2.2 direct the Supplier to end the involvement in the provision of the Services of the relevant person(s).

Employment Indemnity

13.3 The Supplier shall both during and after the Term indemnify the Authority and Service Recipients against all Employee Liabilities that may arise as a result of any claims brought against the Authority or a Service Recipient by any person where such claim arises from any act or omission of the Supplier or any Supplier Personnel.

Income Tax and National Insurance Contributions

13.4 Where the Supplier or any Supplier Personnel are liable to be taxed in the UK or to pay national insurance contributions in respect of consideration received under this Agreement, the Supplier shall:-

13.4.1 at all times comply with the Income Tax (Earnings and Pensions) Act 2003 and all other statutes and regulations relating to income tax, and the Social Security Contributions and Benefits Act 1992 and all other statutes and regulations relating to national insurance contributions, in respect of that consideration; and

13.4.2 indemnify the Authority against any income tax, national insurance and social security contributions and any other liability, deduction, contribution, assessment or claim arising from or made in connection with the provision of the Services by the Supplier or any Supplier Personnel.

Staff Transfer

13.5 The Parties agree that:-

13.5.1 commencement of the provision of the Services or a part of the Services is not anticipated by the Parties to result in a Relevant Transfer and accordingly Part C of Schedule 9.1 (*Staff Transfer*) shall apply; and

13.5.2 Part E of Schedule 9.1 (*Staff Transfer*) shall apply in relation to the expiry or termination of the Services or any part of the Services.

14. SUPPLY CHAIN RIGHTS AND PROTECTIONS

Appointment of Sub-contractors

14.1 The Supplier shall not appoint any Sub-contractor without the Authority's prior written consent.

14.2 Notwithstanding the Supplier's right to sub-contract pursuant to this Clause 14, the Supplier shall remain responsible for all acts and omissions of its Sub-contractors and the acts and omissions of those employed or engaged by the Sub-contractors as if they were its own. In respect of any element of the Services delivered by Supplier Personnel and/or which are Sub-contracted by the Supplier, an obligation on the Supplier to do or to refrain from doing any act or thing under this Agreement, shall include an obligation on the Supplier to procure that the Supplier Personnel and the Sub-contractor also do or refrain from doing such act or thing in their delivery of those elements of the Services.

14.3 An obligation on the Supplier to do, or to refrain from doing, any act or thing shall include an obligation upon the Supplier to procure that all Sub-contractors and Supplier Personnel also do, or refrain from doing, such act or thing.

Supply chain protection

14.4 The Supplier shall ensure that all Sub-contracts (which in this Clause 14.4 includes any contract in the Supplier's supply chain made wholly or substantially for the purpose of performing or contributing to the performance of the whole or any part of this Agreement) contain provisions:-

14.4.1 provisions which will enable the Supplier to discharge its obligations under this Agreement;

14.4.2 where relevant to the Sub-contractor concerned, obligations no less onerous on the Sub-contractor than those imposed on the Supplier under this Agreement in respect of:

(a) data protection requirements set out in Clause 19 (*Authority Data and Security Requirements*) and 22 (*Protection of Personal Data*);

(b) FOIA requirements set out in Clause 21 (*Freedom of Information*);

(c) the conduct of Audits set out in Part 3 of Schedule 7.5 (*Financial Reports and Audit Rights*); and

14.4.3 a provision restricting the ability of the Sub-contractor to sub-contract all or any part of the services provided to the Supplier under the Sub-contract without the Supplier first obtaining the written consent of the Authority.

14.5 The Supplier shall:-

14.5.1 pay any undisputed sums which are due from it to a Sub-contractor within thirty (30) days of verifying that the invoice is valid and undisputed. Such verification to take place within a reasonable period not exceeding ten (10) Working Days following receipt by the Supplier of an invoice from a Sub-contractor;

Termination of Sub-contracts

14.6 The Authority may require the Supplier to terminate a Sub-contract where the acts or omissions of the relevant Sub-contractor have caused or materially contributed to the Authority's right of termination pursuant to Clause 29.1.2 (*Termination by the Authority*).

SECTION F - INTELLECTUAL PROPERTY, DATA AND CONFIDENTIALITY

15. INTELLECTUAL PROPERTY RIGHTS

15.1 Except as expressly set out in this Agreement:-

15.1.1 the Authority shall not acquire any right, title or interest in or to the Intellectual Property Rights of the Supplier or its licensors, namely:

(a) the Supplier Software;

(b) the Third Party Software;

(c) the Third Party IPRs; and

(d) the Supplier IPRs;

15.1.2 the Supplier shall not acquire any right, title or interest in or to the Intellectual Property Rights of the Authority or its licensors, including:-

(a) the Authority Data; and

(b) the Authority Background IPRs.

15.2 Where either Party acquires, by operation of law, title to Intellectual Property Rights that is inconsistent with the allocation of title set out in Clause 15.1, it shall assign in writing such Intellectual Property Rights as it has acquired to the other Party on the request of the other Party (whenever made).

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

16. LICENCES GRANTED BY THE SUPPLIER

Supplier Software and Supplier IPRs

16.1 The Supplier shall not use any Supplier Software in the provision of the Services unless it is detailed in Schedule 5 (*Software*) or has prior approval in writing from the Authority.

16.2 The Supplier hereby grants to the Authority and each Service Recipient a revocable, royalty-free, non-exclusive, non-transferable, and non-sublicensable:

16.2.1 licence to use the Supplier COTS Software, Licensed Data, and Supplier COTS IPRs during the Term on the licence terms identified in a letter in or substantially in the form set out in Appendix 1 to Schedule 5 (*Software*) and signed by or on behalf of the Parties on or before the Effective Date.

(a) during the Term for any purpose relating to the Services and for any purpose relating to the exercise of the Authority's and a Service Recipient's business or function (and including the right for the Authority and Service Recipients to integrate the Licensed Software with the software of Other Suppliers Software and allow data exchange between them providing Authority procures Supplier Integration capabilities); and

(b) during the Data Handover Period for any purpose relating to the extraction and handover of the Authority Data to the Authority and Service Recipients and/or a Replacement Supplier.

Third Party Software and Third Party IPRs

16.3 The Supplier shall not use the in the provision of the Services any Third Party Non-COTS Software or Third Party Non-COTS IPRs unless it is detailed in Schedule 5 (*Software*) or has prior approval in writing from the Authority.

16.4 The Supplier hereby grants (or shall procure that the relevant third party grants) to the Authority and each Service Recipient a royalty free and nonexclusive licence during the Term and Data Handover Period to use the Third Party Non-COTS Software and Third Party Non-COTS IPRs on the terms set out in Clauses **Error! Reference source not found.** and 16.2.1 (*Supplier Software and Supplier IPRs*), subject to the provisions of Clause **Error! Reference source not found.**.

16.5 If the Supplier cannot obtain for the Authority and each Service Recipient a licence in respect of any Third Party Non-COTS Software and/or Third Party Non-COTS IPRs in accordance with the licence terms set out in Clause 16.4, the Supplier shall:

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

16.5.2 use the relevant Third Party Non-COTS Software and/or Third Party Non-COTS IPRs only if the Authority has first approved in writing the terms of the licence from the relevant third party (such terms to be detailed in Schedule 5 (*Software*) for Third Party Non-COTS Software that the Supplier intends to use within the Services as at the Effective Date).

16.6 The Supplier shall:

16.6.1 notify the Authority in writing of all Third Party COTS Software and Third Party COTS IPRs that it uses exclusively for the Authority and the terms on which it uses them (such terms to be detailed in Schedule 5 (*Software*) for Third Party COTS Software that the Supplier intends to use within the Services as at the Effective Date);

Open Source Software

16.7 The Supplier shall ensure that the Software does not contain any Open Source software exclusively for the Authority other than such of the Software as is identified as such in Schedule 5 (*Software*). The Supplier warrants that the Open Source software exclusively for the Authority is licensed upon terms which permit the use of such Open Source software by the Supplier, the Authority and each of the Service Recipients for all purposes contemplated by this Agreement.

Authority's right to assign/novate licences

16.8 The Authority may assign, novate or otherwise transfer its rights and obligations under the licences granted pursuant to Clause 16.2 (*Supplier Software and Supplier IPRs*) to any person to whom this Agreement is assigned, novated or otherwise transferred in accordance with Clause 32 (*Assignment and Novation*).

16.9 Any change in the legal status of the Authority or a Service Recipient shall not affect the validity of any licence granted in this Clause 16.2 (*Supplier Software and Supplier IPRs*) and any successor bodies shall still be entitled to the benefit of any such licence.

17. LICENCES GRANTED BY THE AUTHORITY

17.1 The Authority hereby grants (or shall procure the grant) to the Supplier a royalty -free, non-exclusive, non--transferable licence during the Term to use the Authority Background IPRs and the Authority Data solely to the extent necessary for performing the Services, along with the access of NDA

systems as required, in accordance with this Agreement, including (but not limited to) the right to grant sub-licences to Sub-contractors provided that:-

17.1.1 any relevant Sub-contractor has entered into a confidentiality undertaking with the Authority on the same terms as set out in Clause 20 (*Confidentiality*); and

17.1.2 the Supplier shall not, without the Authority's prior written consent, use the licensed materials for any other purpose or for the benefit of any person other than the Authority and the Service Recipients.

17.1.3 Notwithstanding anything to the contrary contained herein, Supplier and its affiliates (and their successors and assigns) shall have the right to aggregate, normalize, de-identify, and create derivative products and shall wholly own such derivative products provided that no data or the source of such data, can reasonably be attributable back to Authority.

17.2 In the event of the termination or expiry of this Agreement, the licence granted pursuant to Clause 17.1 and any sub-licence granted by the Supplier in accordance with Clause 17.1 shall terminate automatically on the date of such termination or expiry and the Supplier shall:-

17.2.1 immediately cease all use of the Authority Background IPRs and the Authority Data (as the case may be);

17.2.2 at the discretion of the Authority, return or destroy documents and other tangible materials that contain any of the Authority Background IPRs and the Authority Data, provided that if the Authority has not made an election within six (6) months of the termination of the licence, the Supplier may destroy the documents and other tangible materials that contain any of the Authority Background IPRs and the Authority Data (as the case may be); and

17.2.3 ensure, so far as reasonably practicable, that any Authority Background IPRs and Authority Data that are held in electronic, digital or other machine -readable form ceases to be readily accessible from any Supplier computer, word processor, voicemail system or any other Supplier device containing such Authority Background IPRs and/or Authority Data.

18. IPRS INDEMNITY

18.1 The Supplier shall at all times, during and after the Term, on written demand indemnify the Authority and each other Indemnified Person, and keep the Authority and each other Indemnified Person indemnified, against all Losses incurred by, awarded against or agreed to be paid by an Indemnified Person arising from an IPRs Claim.

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

18.2.1 procure for the Authority or other relevant Indemnified Person the right to continue using the relevant item which is subject to the IPRs Claim; or

18.2.2 replace or modify the relevant item with non--infringing substitutes provided that:-

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

(b) the replaced or modified item does not have an adverse effect on any other services or the IT Environment;

(c) there is no additional cost to the Authority or relevant Indemnified Person (as the case may be); and

(d) the terms and conditions of this Agreement shall apply to the replaced or modified Services.

18.3 If the Supplier elects to procure a licence in accordance with Clause 18.2.1 or to modify or replace an item pursuant to Clause 18.2.2, but this has not avoided or resolved the IPRs Claim, then:-

18.3.1 the Authority may terminate this Agreement (if subsisting) with immediate effect by written notice to the Supplier; and

18.3.2 without prejudice to the indemnity set out in Clause 18.1, the Supplier shall be liable for all reasonable and unavoidable costs of the substitute items and/or services including the additional costs of procuring, implementing and maintaining the substitute items.

19. AUTHORITY DATA AND SECURITY REQUIREMENTS

19.1 The Supplier shall not delete or remove any proprietary notices contained within or relating to the Authority Data.

19.2 The Supplier shall not store, copy, disclose, or use the Authority Data except as necessary for the performance by the Supplier of its obligations under this Agreement or as otherwise expressly authorised in writing by the Authority.

19.3 To the extent that Authority Data is held and/or processed by the Supplier, the Supplier shall supply that Authority Data to the Authority or relevant Service Recipient as requested by the Authority and in a standard format such as a .CSV file or any other mutually agreed upon format.

19.4 The Supplier shall preserve the integrity of Authority Data and prevent the corruption or loss of Authority Data at all times that the relevant Authority Data is under its control or the control of any Sub-contractor.

19.5 The Supplier shall perform secure back-ups of all Authority Data and shall ensure that up-to-date back-ups are stored off-site in accordance with the Service Continuity Plan and in any event not less than once in every twenty four (24) hours, seven (7) days a week.

19.6 The Supplier shall ensure that any system on which the Supplier holds any Authority Data, including back-up data, is a secure system that complies with the Security Requirements.

19.7 If the Authority Data is corrupted, lost or sufficiently degraded as a result of the Supplier's Default so as to be unusable, the Authority may:-

19.7.1 require the Supplier (at the Supplier's expense) to restore or procure the restoration of Authority Data to the extent and in accordance with the requirements specified in Schedule 8.6 (*Service Continuity Plan*) and the Supplier shall do so as soon as practicable but not later than five (5) Working Days from the date of receipt of the Authority's notice; and/or

19.8 If at any time the Supplier suspects or has reason to believe that Authority Data has or may become corrupted, lost or sufficiently degraded in any way for any reason, then the Supplier shall notify the Authority immediately and inform the Authority of the remedial action the Supplier proposes to take.

19.9 The Supplier shall comply with the requirements of Schedule 2.4 (*Security Management*).

19.10 The Authority shall notify the Supplier of any changes or proposed changes to the Baseline Security Requirements.

19.11 If the Supplier believes that a change or proposed change to the Baseline Security Requirements will have a material and unavoidable cost implication to the Services it may submit a Change Request. In doing so, the Supplier must support its request by providing evidence of the cause of any increased costs and the steps that it has taken to mitigate those costs. Any change to the Charges shall then be agreed in accordance with the Change Control Procedure.

19.12 Until and/or unless a change to the Charges is agreed by the Authority pursuant to Clause 19.11 the Supplier shall continue to perform the Services in accordance with its existing obligations.

Malicious Software

19.13 The Supplier shall, as an enduring obligation throughout the Term, use the latest versions of anti-virus definitions and software available from an industry accepted anti-virus software vendor (unless otherwise agreed in writing between the Parties) to check for, contain the spread of, and minimise the impact of Malicious Software in the Supplier System (or as otherwise agreed by the Parties).

19.14 Notwithstanding Clause 19.13 (*Malicious Software*), if Malicious Software is found, the Parties shall co-operate to reduce the effect of the Malicious Software and, particularly if Malicious Software causes loss of operational efficiency or loss or corruption of Authority Data, assist each other to mitigate any Losses and to restore the Supplier's provision of the Services in accordance with this Agreement, to the Authority's desired operating efficiency.

19.15 Any cost arising out of the actions of the Parties taken in compliance with the provisions of Clause 19.14 (*Malicious Software*) shall be borne by the Parties as follows:

19.15.1 by the Supplier where the Malicious Software has been introduced into the Supplier System by the Supplier or its Sub-contractors, including through Third Party Software, (except where the Authority has waived the obligation set out in Clause 19.13 (*Malicious Software*) or originates from the Authority Data (whilst the Authority 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 Authority when provided to the Supplier; and

19.15.2 otherwise by the Authority.

20. CONFIDENTIALITY

20.1 For the purposes of this Clause 20, the term "Disclosing Party" shall mean a Party (including for the purposes of this Clause 20 (*Confidentiality*), only, each Service Recipient) which discloses or makes available directly or indirectly its Confidential Information and "Recipient" shall mean the Party (including for the purposes of this Clause 20 (*Confidentiality*), only, each Service Recipient) which receives or obtains directly or indirectly Confidential Information.

20.2 Except to the extent set out in this Clause 20 or where disclosure is expressly permitted elsewhere in this Agreement, the Recipient shall:-

20.2.1 treat the Disclosing Party's Confidential Information as confidential and keep it in secure custody (which is appropriate depending upon the form in which such materials are stored and the nature of the Confidential Information contained in those materials);

20.2.2 not disclose the Disclosing Party's Confidential Information to any other person except as expressly set out in this Agreement or without obtaining the owner's prior written consent;

20.2.3 not use or exploit the Disclosing Party's Confidential Information in any way except for the purposes anticipated under this Agreement; and

20.2.4 immediately notify the Disclosing Party if it suspects or becomes aware of any unauthorised access, copying, use or disclosure in any form of any of the Disclosing Party's Confidential Information.

20.3 The Recipient shall be entitled to disclose the Confidential Information of the Disclosing Party where:-

20.3.1 the Recipient is required to disclose the Confidential Information by Law, provided that Clause 21 (*Transparency and Freedom of Information*) shall apply to disclosures required under the FOIA or the EIRs;

20.3.2 the need for such disclosure arises out of or in connection with:-

(a) any legal challenge or potential legal challenge against the Authority arising out of or in connection with this Agreement;

(b) the examination and certification of the Authority's or a Service Recipient's accounts (provided that the disclosure is made on a confidential basis) or for any examination pursuant to section 6(1) of the National Audit Act 1983 of the economy, efficiency and effectiveness with which the Authority or a Service Recipient is making use of any Services provided under this Agreement; or

(c) the conduct of a Central Government Body review in respect of this Agreement; or

20.3.3 the Recipient has reasonable grounds to believe that the Disclosing Party is involved in activity that may constitute a criminal offence under the Bribery Act 2010 and the disclosure is being made to the Serious Fraud Office.

20.4 If the Recipient is required by Law to make a disclosure of Confidential Information, the Recipient shall as soon as reasonably practicable and to the extent permitted by Law notify the Disclosing Party of the full circumstances of the required disclosure including the relevant Law and/or regulatory body requiring such disclosure and the Confidential Information to which such disclosure would apply.

20.5 The Supplier may disclose the Confidential Information of the Authority or a Service Recipient on a confidential basis only to:-

20.5.1 Supplier Personnel who are directly involved in the provision of the Services and need to know the Confidential Information to enable performance of the Supplier's obligations under this Agreement;

20.5.2 its auditors; and

20.5.3 its professional advisers for the purposes of obtaining advice in relation to this Agreement.

Where the Supplier discloses Confidential Information of the Authority or a Service Recipient pursuant to this Clause 20.5, it shall remain responsible at all times for compliance with the confidentiality obligations set out in this Agreement by the persons to whom disclosure has been made.

20.6 The Authority and each Service Recipient may disclose the Confidential Information of the Supplier:-

20.6.1 on a confidential basis to any Central Government Body for any proper purpose of the Authority, the Service Recipient or of the relevant Central Government Body;

20.6.2 to Parliament and Parliamentary Committees or if required by any Parliamentary reporting requirement;

20.6.3 to the extent that the Authority or Service Recipient (acting reasonably) deems disclosure necessary or appropriate in the course of carrying out its public functions;

20.6.4 on a confidential basis to a professional adviser, consultant, supplier or other person engaged by any of the entities described in Clause 20.6.1 for any purpose relating to or connected with this Agreement;

20.6.5 on a confidential basis for the purpose of the exercise of its rights under this Agreement, including the Audit Rights and Exit Management rights;

20.6.6 on a confidential basis to a proposed Successor Body in connection with any assignment, novation or disposal of any of its rights, obligations or liabilities under this Agreement;

20.6.7 between Service Recipients and the Authority and vice versa; and/or

20.6.8 to any Other Supplier, on a confidential basis, with prior written agreement of the Supplier

and for the purposes of the foregoing, references to disclosure on a confidential basis shall mean disclosure subject to a confidentiality agreement or arrangement containing terms no less stringent than those placed on the Authority and Service Recipients under this Clause 20.

20.7 Nothing in this Clause 20 shall prevent a Recipient from using any techniques, ideas or know-how gained during the performance of this Agreement in the course of its normal business to the extent that this use does not result in a disclosure of the Disclosing Party's Confidential Information or an infringement of Intellectual Property Rights.

21. TRANSPARENCY AND FREEDOM OF INFORMATION

21.1 In order to comply with the Government's policy on transparency in the areas of procurement and contracts the Supplier agrees that the Agreement and the Tender Documents will be published by the Authority on a designated web site save where to do so would disclose information the disclosure of which would:

21.1.1 contravene the provisions of Clause 20 (*Confidentiality*);

21.1.2 be contrary to regulation 21 of the Public Contracts Regulations 2015; or

21.1.3 in the reasonable opinion of the Authority be prevented by virtue of one or more of the exemptions in the Freedom of Information Act 2000 or one or more of the exceptions in the Environmental Information Regulations 2004.

21.2 If any of the situations in Clauses 21.1.1 to 21.1.3 apply, the Supplier consents to the Agreement or Tender Documents being redacted by the Authority to the extent necessary to remove or obscure the relevant material and being published on the designated website subject to those redactions.

21.3 In order to comply with the Government's policy on transparency in the area of contract performance the Supplier agrees that performance against KPI 1, KPI 5, and KPI 6 of Schedule 2.2 (*Performance Levels*) will be published by the Authority on a designated web site save where to do so would disclose information the disclosure of which would:

21.3.1 contravene the provisions of Clause 20 (*Confidentiality*);

21.3.2 be contrary to regulation 21 of the Public Contracts Regulations 2015; or

21.3.3 in the reasonable opinion of the Authority be prevented by virtue of one or more of the exemptions in the Freedom of Information Action 2000 or one or more of the exceptions in the Environmental Information Regulations 2004.

21.4 The Authority shall agree with the Supplier the Supplier's performance against KPI 1, KPI 5 and KPI 6 in advance of any publication.

21.5 The Supplier acknowledges that the Authority and Service Recipients are subject to the requirements of the FOIA and the EIRs. The Supplier shall:-

21.5.1 provide all necessary assistance and cooperation as reasonably requested by the Authority and Service Recipients to enable the Authority and Service Recipients to comply with its obligations under the FOIA and EIRs;

21.5.2 transfer to the Authority (or at the Authority's request the relevant Service Recipient) all Requests for Information relating to this Agreement that it receives as soon as practicable and in any event within five (5) Working Days of receipt or sooner wherever possible;

21.5.3 provide the Authority (or at the Authority's request the relevant Service Recipient) with a copy of all Information held on behalf of the Authority and Service Recipients which is requested in a Request For Information and which is in its possession or control in the form that the Authority or Service Recipient requires within five (5) Working Days (or such other period as the Authority or Service Recipient may reasonably specify) of the Authority's or Service Recipient's request for such Information; and

21.5.4 not respond directly to a Request For Information addressed to the Authority or a Service Recipient unless authorised in writing to do so by the Authority.

21.6 The Supplier acknowledges that the Authority or a Service Recipient may be required under the FOIA and EIRs to disclose Information (including Commercially Sensitive Information) without consulting or obtaining consent from the Supplier. The Authority or Service Recipient shall take reasonable steps to notify the Supplier of a Request For Information (in accordance with the Secretary of State's section 45 Code of Practice on the Discharge of the Functions of Public Authorities under Part 1 of the FOIA) to the extent that it is permissible and reasonably practical for it to do so but (notwithstanding any other provision in this Agreement) the Authority or Service Recipient shall be responsible for determining in its absolute discretion whether any information (including Commercially Sensitive Information) is exempt from disclosure in accordance with the FOIA and EIRs.

22. PROTECTION OF PERSONAL DATA

Arrangement between the Parties

22.1 The Parties acknowledge that the factual arrangement between them dictates the classification of each Party in respect of the Data Protection Legislation. Notwithstanding the foregoing, the Parties anticipate that during the term of the Agreement:-

22.1.1 the Authority and/or applicable Service Recipient shall be the Controller of the (i) Authority Personal Data, (ii) Authority's Contact Data for its own internal business purposes and (ii) where it is Processed by the Authority in accordance with Clause 22.2, the Supplier's Contact Data;

22.1.2 the Supplier shall be the Controller of the (i) Supplier's Contact Data for its own internal business purposes and (ii) where the Authority's Contact Data is Processed by it in accordance with Clause 22.2, the Authority's Contact Data; and

22.1.3 the Supplier shall be the Processor in relation to its Processing of the Authority Personal Data as described in the Appendix to the Supplier Solution which have been made available to the Supplier by the Authority (whether directly or indirectly) for the purpose of performing the services.

22.2 The Parties each acknowledge and agree that they may need to Process Contact Data (in their respective capacities as Controllers) in order to (as appropriate): (a) administer and provide the Services; (b) request and receive the Services; (c) compile, dispatch and manage the payment of invoices relating to the Services; (d) manage the Agreement and resolve any disputes relating to it; (e) respond and/or raise general queries relating to the Services; and (f) comply with their respective regulatory and other compliance obligations.

22.3 Each Party shall Process the other Party's Contact Data for the purposes set out in Clause 22.2 in accordance with their respective privacy policies. The Parties acknowledge that they may be required to share the other Party's Contact Data with their Affiliates and other relevant parties, within the UK, in order to carry out the activities listed in Clause 22.2, and in doing so each Party will ensure that the sharing and use of this Contact Data complies with applicable Data Protection Legislation.

22.4 The Supplier shall comply at all times with the DPA and shall not perform its obligations under this Agreement in such a way as to cause the Supplier or the Authority or Service Recipients to breach any of their respective obligations under the DPA.

22.5 Each of the Parties acknowledges and agrees that the Appendix to the Supplier Solution contains an accurate description of the following where the Supplier is acting as a Processor on behalf of the Authority and/or Service Recipients:-

the subject matter of the Processing;

the duration of the Processing;

the nature and purpose of the Processing;

the type of Personal Data being Processed; and

the categories of Data Subjects.

22.6 The Parties agree that the Standard Contractual Clauses as provided in Schedule 10 (Standard Contractual Clauses) shall be incorporated and shall form part of this Agreement as the applicable appropriate safeguard for any transfers of Personal Data outside of the UK between the Parties pursuant to Clause 22.2 above and the Supplier shall ensure that any such onward transfers of such Personal Data are also subject to Standard Contractual Clauses.

Processor Obligations

22.7 Where the Supplier is processing Personal Data as a Processor for the Authority and/or Service Recipients, the Supplier shall:-

22.7.1 process the Personal Data only for the purpose of performing its obligations under this Agreement or otherwise on the instructions of the Authority or relevant Service Recipient. Unless prohibited by law, if the Supplier is required by UK Law to act other than in accordance with the instructions of the Authority or relevant Service Recipient, the Supplier shall (unless prohibited by such law) promptly, and in any event within twenty-four (24) hours of becoming aware of the same, notify the Authority and relevant Service Recipient;

22.7.2 hold the Authority Personal Data it is processing on behalf of the Authority and/or Service Recipients logically separated from other data or information processed by the Supplier;

22.7.3 implement appropriate technical and organisational measures to safeguard the Personal Data against unauthorised or unlawful processing and against accidental loss, destruction, damage, alteration or disclosure which are sufficient to comply with the obligations placed upon Authority or Service Recipient (as Controller) and the Supplier (as Processor) in accordance with the Data Protection Legislation and those under this Agreement (including the measures set out in the Authority Requirements) and upon request provide to the Authority evidence of its compliance with such requirements;

22.7.4 ensure that all employees or agents required to access the Personal Data are informed of the confidential nature of the Personal Data and have entered into an appropriate contractual agreement that requires them to keep the Personal Data confidential;

22.7.5 not sub-contract any Processing of the Personal Data, replace an existing sub-contractor who is Processing the Personal Data or alter the scope or location of Processing carried out by an existing sub-contractor (a "**sub-processing change**") unless all of the following have been met:-

(a) the Supplier has given the Authority not less than sixty (60) days' written notice of the relevant sub-processing change;

(b) the Supplier has undertaken due diligence on the sub-contractor with all due skill and care, including a risk assessment of the information governance related practices and processes of the sub-contractor and has established that the outcome of the due diligence is a determination that the sub-contractor and the

arrangements made for the sub-processing would objectively be adequate and sufficient to ensure compliance with the applicable requirements of the DPA, and has given notice of the outcome to the Authority;

(c) the Supplier undertakes to ensure that the sub-processing contract will be on terms that are substantially the same as the terms set out in this Clause 22; and

(d) the Authority has not objected to the use of the sub-processor within the period of notice provided by the Supplier (or if longer, the period of sixty (60) days following service of notice);

22.7.6 notify the Authority promptly (and in any event within five (5) Working Days) following its receipt from a Data Subject, the Information Commissioner or any third party of a request, complaint, communication or Regulator Correspondence and:-

(a) not disclose any Personal Data in response to any such request or correspondence without the consent of the Authority;

(b) provide the Authority with full co-operation and assistance (including providing copies of all data held) as required by the Authority in relation to any such complaint or request made or Regulator Correspondence received; and

(c) provide data promptly and so as to enable the Authority and each Service Recipient to comply with any relevant timescales set out in the Data Protection Legislation and otherwise in accordance with the Authority's and relevant Service Recipient's instructions;

22.7.7 notify the Authority promptly and in any event within twelve (12) hours upon becoming aware of any actual or suspected breach of Clause 22.7.3 and:-

(a) promptly provide the Authority with a report containing all the circumstances and details in relation to the Personal Data breach, including those specified in Article 33(3) of the GDPR;

(b) assist the Authority and Service Recipients to make any notifications to the Information Commissioner and affected Data Subjects and co-operate with the Authority, Service Recipients, the Information Commissioner and any other regulatory bodies as required;

(c) provide any information requested by the Authority, Service Recipients, the Information Commissioner and/or any other regulatory bodies in relation to the breach;

(d) investigate the incident and its cause;

(e) seek to recover the compromised data and as soon as practicable and implement any measures necessary to restore the security of the Personal Data;

(f) comply with all applicable guidance (including Information Commissioner guidance);

(g) co-ordinate with the Authority with respect to the management of public relations and public statements relating to the incident and make no public statement in relation to the incident unless the Authority has provided its specific written consent to such statement;

22.7.8 provide the Authority with full cooperation and assistance to ensure compliance with its obligations under the DPA including:-

(a) obligations relating to the security and integrity of the Personal Data; and

(b) undertaking any data protection impact assessments (as required by the DPA);

22.7.9 notify the Authority immediately if it considers in its opinion any of its instructions infringe the DPA;

22.7.10 not transfer any Personal Data outside the United Kingdom except as permitted by the Authority in writing and, in granting consent to the transfer, the Authority may impose additional terms on the Processing of the Personal Data on the Supplier and/or the data importer (as applicable), including incorporating the Standard Contractual Clauses and/or a direct data processing agreement.

22.7.11 upon the expiry or termination of the Agreement or otherwise at any time where required by at Authority's option or direction, arrange for the prompt and safe return and/or secure permanent destruction (in accordance with HMG IA Standard No. 5 Secure Sanitisation of Protectively Marked or Sensitive Information) of any and/or all Authority Personal Data, together with all copies in its or its sub-contractors' possession or control within seven (7) days and, where requested by the Authority, certify that such destruction has taken place.

22.8 By signing this Agreement, the Authority is authorizing the Supplier to store Personal Data on servers located in data centres owned and controlled by the Supplier or by a third-party processor acting on the Supplier's behalf in the United States of America (which involves transfers of Personal Data outside of the UK). The Parties agree that the Standard Contractual Clauses as provided in Schedule 10 (Standard Contractual Clauses) shall be incorporated and shall form part of this Agreement as the applicable appropriate safeguard for any transfers of Personal Data outside of the UK between the Parties including those described in this clause 22.8.

Variation

22.9 If at any time, in the Authority's opinion, the Authority needs to amend this Agreement in order to comply with its obligations under Data Protection Legislation, including Article 28 of the GDPR, the Supplier agrees to enter into a written variation of this Agreement to make the amendments which in the Authority's opinion are required. In the event such amendments are not able to be agreed, the Parties acknowledge and agree that no further Processing of the Personal Data under this Agreement will be carried out until such variation has been agreed and executed unless directed otherwise by the Authority in writing and then in those circumstances the Supplier may only continue to Process Authority Data in accordance with the Authority's written directions

23. PUBLICITY AND BRANDING

23.1 The Supplier shall not:-

23.1.1 make any press announcements or publicise this Agreement or its contents in any way; or

23.1.2 use the Authority's or a Service Recipient's name or brand in any promotion or marketing or announcement of orders,

without the prior written consent of the Authority, which shall not be unreasonably withheld or delayed.

23.2 Each Party acknowledges to the other that nothing in this Agreement either expressly or by implication constitutes an endorsement of any products or services of the other Party (including the Services, the Supplier System and the Authority System) and each Party agrees not to conduct itself in such a way as to imply or express any such approval or endorsement.

SECTION G - LIABILITY, INDEMNITIES AND INSURANCE

24. LIMITATIONS ON LIABILITY

Unlimited liability

24.1 Neither Party limits its liability for:-

24.1.1 death or personal injury caused by its negligence, or that of its employees, agents or Sub-contractors (as applicable);

24.1.2 fraud or fraudulent misrepresentation by it or its employees;

24.1.3 breach of any obligation as to title implied by section 12 of the Sale of Goods Act 1979 or section 2 of the Supply of Goods and Services Act 1982; or

24.1.4 any liability to the extent it cannot be limited or excluded by Law.

24.2 The Supplier's liability in respect of the indemnities in Clause 9.5 (VAT), Clause 13.3 (*Employment Indemnity*) and Clause 13.4 (*Income Tax and National Insurance Contributions*) shall be unlimited.

Financial and other limits

24.3 Subject to Clauses 24.1 and 24.2 (*Unlimited Liability*) and Clauses 24.5 and 24.6 (*Consequential losses*):-

24.3.1 the Supplier's aggregate liability in respect of loss of or damage to the Authority Premises or other property or assets of the Authority or a Service Recipient (including technical infrastructure, assets or equipment but excluding any loss or damage to the Authority Data or any other data) that is caused by Defaults of the Supplier occurring in each and any Contract Year shall in no event exceed £2,000,000 (two million pounds) in combined coverage.

24.3.2 The Supplier's aggregate liability in respect of Clause 18 (*IPRs Indemnity*) that is caused by Default of the Supplier occurring in each and any Contract Year shall in no event exceed £3,000,000 (three million pounds);

24.3.3 In no event shall Supplier or its Officers, Directors, Affiliates, Assigns, Agents, Employees, or licensors be liable for any: indirect, incidental, punitive, consequential, special or exemplary damages of any kind or nature whatsoever, including without limitation, lost profits, loss of business, loss of revenues, loss, interruption or corruption of data, computer failure or malfunction, regardless of the cause of action and regardless of the whether such party was advised of the possibility of such damages, The total liability of Resilinc or its licensors under this Agreement shall in no way exceed the three times the aggregate amount paid by the Authority to Supplier for the services giving rise to such liability during the twelve (12) month period immediately preceding the claim; however, such limitation of liability shall not apply to the indemnification obligations set forth in clause 24.3.1 and 24.3.2.

24.3.4 the Supplier's aggregate liability in respect of all other Losses incurred by the Authority and Service Recipients under or in connection with this Agreement as a result of Defaults by the Supplier shall in no event exceed:-

(a) three times the aggregate amount paid by the Authority to Supplier for the services giving rise to such liability during the twelve (12) month period immediately preceding the claim.

(b) in relation to Defaults occurring after the end of the Term, an amount equal to £1,500,000 (one million five hundred thousand pounds).

24.4 Subject to Clause 24.1 (*Unlimited Liability*) and Clause 24.5 (*Consequential Losses*) and without prejudice to the Authority's obligation to pay the Charges as and when they fall due for payment:

24.4.1 the Authority's and Service Recipients' total aggregate liability in respect of all Losses incurred by the Supplier under or in connection with this Agreement as a result of early termination of this Agreement by the Authority pursuant to Clause 29.1.1 (*Termination by the Authority*) or by the Supplier pursuant to Clause 29.3 (*Termination by the Supplier*) shall in no event exceed the following amounts:-

(a) for a termination taking effect prior to the expiry of the first Contract Year, £1,500,000 (one million five thousand pounds); and

(b) for a termination taking effect on and following such expiry, zero; and

24.4.2 the Authority's and Service Recipients' aggregate liability in respect of all Losses incurred by the Supplier under or in connection with this Agreement as a result of Defaults of the Authority shall in no event exceed £1,500,000 (one million five hundred thousand pounds).

Consequential Losses

24.5 Subject to Clauses 24.1 and 24.2 (*Unlimited Liability*) and Clause 24.6, neither Party shall be liable to the other Party for:-

24.5.1 any indirect, special or consequential Loss; or

24.5.2 any loss of profits, turnover, business opportunities or damage to goodwill (in each case whether direct or indirect).

24.6 Notwithstanding Clause 24.5 but subject to Clause 24.3, the Supplier acknowledges that the Authority and Service Recipients may, amongst other things, recover from the Supplier the additional cost of procuring Replacement Services for the remainder of the Term and/or replacement Deliverables, which shall include any incremental costs associated with such Replacement Services above those which would have been payable under this Agreement to the extent that they arise as a result of a Default by the Supplier.

24.7 Where under this Agreement one Party indemnifies the other Party, the Parties shall comply with the provisions of Schedule 8.7 (*Conduct of Claims*) in relation to the conduct of claims made by a third person against the Party having (or claiming to have) the benefit of the indemnity.

Mitigation

24.8 Each Party shall use all reasonable endeavours to mitigate any loss or damage suffered arising out of or in connection with this Agreement, including any Losses for which the relevant Party is entitled to bring a claim against the other Party pursuant to the indemnities in this Agreement.

25. INSURANCE

The Supplier shall comply with the provisions of Schedule 2.5 (*Insurance Requirements*) in relation to obtaining and maintaining insurance.

SECTION H – REMEDIES AND RELIEF

26. RECTIFICATION PLAN PROCESS

26.1 In the event that:-

26.1.1 there is, or is reasonably likely to be, a Delay;

26.1.2 any failure of the Supplier to remedy any breach of its obligations in Clause 5.6.1 and Clauses 5.6.3 to 5.6.7 inclusive within twenty (20) Working Days of becoming aware of the breach or being notified of the breach by the Authority;

26.1.3 in any Service Period there has been:-

(a) a Material KPI Failure; and/or

(b) the Supplier commits a material Default that is capable of remedy (and for these purposes a material Default may be a single material Default or a number of Defaults or repeated Defaults (whether of the same or different obligations and regardless of whether such Defaults are remedied) which taken together constitute a material Default),

(each a "**Notifiable Default**"), the Supplier shall notify the Authority of the Notifiable Default as soon as practicable but in any event within five (5) Working Days of becoming aware of the Notifiable Default, detailing the actual or anticipated effect of the Notifiable Default and, unless the Notifiable Default also constitutes a Rectification Plan Failure or other Supplier Termination Event, the Authority may not terminate this Agreement in whole or in part on the grounds of the Notifiable Default without first following the Rectification Plan Process.

Notification

26.2 If:-

26.2.1 the Supplier notifies the Authority pursuant to Clause 26.1 that a Notifiable Default has occurred; or

26.2.2 the Authority notifies the Supplier that it considers that a Notifiable Default has occurred (setting out sufficient detail so that it is reasonably clear what the Supplier has to rectify),

then, unless the Notifiable Default also constitutes a Supplier Termination Event and the Authority serves a Termination Notice, the Supplier shall comply with the Rectification Plan Process.

26.3 The "**Rectification Plan Process**" shall be as set out in Clauses 26.4 (*Submission of the draft Rectification Plan*) to 27.9 (*Agreement of the Rectification Plan*).

Submission of the draft Rectification Plan

26.4 The Supplier shall submit a draft Rectification Plan to the Authority for it to review as soon as possible and in any event within ten (10) Working Days (or such other period as may be agreed between the Parties) after the original notification pursuant to Clause 26.2 (*Notification*). The Supplier shall submit a draft Rectification Plan even if the Supplier disputes that it is responsible for the Notifiable Default.

26.5 The draft Rectification Plan shall set out:-

26.5.1 full details of the Notifiable Default that has occurred, including a root cause analysis;

26.5.2 the actual or anticipated effect of the Notifiable Default; and

26.5.3 the steps which the Supplier proposes to take to rectify the Notifiable Default (if applicable) and to prevent such Notifiable Default from recurring, including timescales for such steps and for the rectification of the Notifiable Default (where applicable).

26.6 The Supplier shall promptly provide to the Authority any further documentation that the Authority reasonably requires to assess the Supplier's root cause analysis. If the Parties do not agree on the root cause set out in the draft Rectification Plan, either Party may refer the matter to be determined by an expert in accordance with paragraph 6 of Schedule 8.3 (*Dispute Resolution Procedure*).

Agreement of the Rectification Plan

26.7 The Authority may reject the draft Rectification Plan by notice to the Supplier if, acting reasonably, it considers that the draft Rectification Plan is inadequate, for example because the draft Rectification Plan:-

26.7.1 is insufficiently detailed to be capable of proper evaluation;

26.7.2 will take too long to complete;

26.7.3 will not prevent reoccurrence of the Notifiable Default; and/or

26.7.4 will rectify the Notifiable Default but in a manner which is unacceptable to the Authority.

26.8 The Authority shall notify the Supplier whether it consents to the draft Rectification Plan as soon as reasonably practicable. If the Authority rejects the draft Rectification Plan, the Authority shall give reasons for its decision and the Supplier shall take the reasons into account in the preparation of a revised Rectification Plan. The Supplier shall submit the revised draft of the Rectification Plan to the Authority for review within five (5) Working Days (or such other period as agreed between the Parties) of the Authority's notice rejecting the first draft.

26.9 If the Authority consents to the Rectification Plan:-

26.9.1 the Supplier shall immediately start work on the actions set out in the Rectification Plan; and

26.9.2 the Authority may no longer terminate this Agreement in whole or in part on the grounds of the relevant Notifiable Default.

27. AUTHORITY CAUSE

27.1 Notwithstanding any other provision of this Agreement, if the Supplier has failed to:-

27.1.1 Achieve a Milestone by its Milestone Date;

27.1.2 provide the Operational Services in accordance with the Target Performance Levels; and/or

27.1.3 comply with its obligations under this Agreement,

(each a "**Supplier Non-Performance**"),

and can demonstrate that the Supplier Non-performance- would not have occurred but for an Authority Cause, then (subject to the Supplier fulfilling its obligations in this Clause 27):-

(a) the Supplier shall not be treated as being in breach of this Agreement to the extent the Supplier can demonstrate that the Supplier Non-performance- was caused by the Authority Cause;

(b) the Authority shall not be entitled to exercise any rights that may arise as a result of that Supplier Non-performance- to terminate this Agreement pursuant to Clause 29.1.2 (*Termination by the Authority*);

(c) where the Supplier Non-performance- constitutes the failure to Achieve a Milestone by its Milestone Date:-

(i) the Milestone Date shall be postponed by a period equal to the period of Delay that the Supplier can demonstrate was caused by the Authority Cause; and

(ii) if the Authority, acting reasonably, considers it appropriate, the Implementation Plan shall be amended to reflect any consequential revisions required to subsequent Milestone Dates resulting from the Authority Cause; and/or

(d) where the Supplier Non-performance- constitutes a Performance Failure:-

(i) the Supplier shall not be liable to accrue Service Credits; and

(ii) the Supplier shall be entitled to invoice for the Service Charges for the relevant Operational Services affected by the Authority Cause,

in each case, to the extent that the Supplier can demonstrate that the Performance Failure was caused by the Authority Cause.

27.2 In order to claim any of the rights and/or relief referred to in Clause 27.1, the Supplier shall as soon as reasonably practicable (and in any event within ten (10) Working Days) after becoming aware that an Authority Cause has caused, or is reasonably likely to cause, a Supplier Non-performance-, give the Authority notice (a "**Relief Notice**") setting out details of:-

27.2.1 the Supplier Non-performance-;

27.2.2 the Authority Cause and its effect, or likely effect, on the Supplier's ability to meet its obligations under this Agreement;

27.2.3 any steps which the Authority can take to eliminate or mitigate the consequences and impact of such Authority Cause; and

27.2.4 the relief claimed by the Supplier.

27.3 Following the receipt of a Relief Notice, the Authority shall as soon as reasonably practicable consider the nature of the Supplier Non-performance- and the alleged Authority Cause and whether it agrees with the Supplier's assessment set out in the Relief Notice as to the effect of the relevant Authority Cause and its entitlement to relief, consulting with the Supplier where necessary.

27.4 The Supplier shall use all reasonable endeavours to eliminate or mitigate the consequences and impact of an Authority Cause, including the duration and consequences of any Delay or anticipated Delay.

27.5 Without prejudice to Clause 5.8 (*Continuing obligation to provide the Services)*, if a Dispute arises as to:-

27.5.1 whether a Supplier Non-performance- would not have occurred but for an Authority Cause; and/or

27.5.2 the nature and/or extent of the relief claimed by the Supplier,

either Party may refer the Dispute to the Dispute Resolution Procedure. Pending the resolution of the Dispute, both Parties shall continue to resolve the causes of, and mitigate the effects of, the Supplier Non-performance-.

27.6 Any Change that is required to the Implementation Plan or to the Charges pursuant to this Clause 27 shall be implemented in accordance with the Change Control Procedure.

28. FORCE MAJEURE

28.1 Subject to the remaining provisions of this Clause 28 (and, in relation to the Supplier, subject to its compliance with its obligations in Schedule 8.6 (*Service Continuity Plan*)), a Party may claim relief under this Clause 28 from liability for failure to meet its obligations under this Agreement for as long as and only to the extent that the performance of those obligations is directly affected by a Force

Majeure Event. Any failure or delay by the Supplier in performing its obligations under this Agreement which results from a failure or delay by an agent, Sub-contractor or supplier shall be regarded as due to a Force Majeure Event only if that agent, Sub-contractor or supplier is itself impeded by a Force Majeure Event from complying with an obligation to the Supplier.

28.2 The Affected Party shall as soon as reasonably practicable issue a Force Majeure Notice, which shall include details of the Force Majeure Event, its effect on the obligations of the Affected Party and any action the Affected Party proposes to take to mitigate its effect.

28.3 If the Supplier is the Affected Party, it shall not be entitled to claim relief under this Clause 28 to the extent that consequences of the relevant Force Majeure Event:-

28.3.1 are capable of being mitigated by any of the Services including the Service Continuity Services and the obligation to ensure that the Software complies with the security requirements under this Agreement (including with respect to the security of the Authority Data), but the Supplier has failed to do so; and/or

28.3.2 should have been foreseen and prevented or avoided by a prudent provider of services similar to the Services, operating to the standards required by this Agreement.

28.4 Subject to Clause 28.5, as soon as practicable after the Affected Party issues the Force Majeure Notice, and at regular intervals thereafter, the Parties shall consult in good faith and use reasonable endeavours to agree any steps to be taken and an appropriate timetable in which those steps should be taken, to enable continued provision of the Services affected by the Force Majeure Event.

28.5 The Parties shall at all times following the occurrence of a Force Majeure Event and during its subsistence use their respective reasonable endeavours to prevent and mitigate the effects of the Force Majeure Event. Where the Supplier is the Affected Party, it shall take all steps in accordance with Good Industry Practice to overcome or minimise the consequences of the Force Majeure Event.

28.6 Where, as a result of a Force Majeure Event:-

28.6.1 an Affected Party fails to perform its obligations in accordance with this Agreement, then during the continuance of the Force Majeure Event:-

(a) where the Affected Party is the Supplier, the Authority shall not be entitled to exercise any rights to terminate this Agreement in whole or in part as a result of such failure other than pursuant to Clause 29.1.3 (Termination by the Authority); and

(b) neither Party shall be liable for any Default arising as a result of such failure;

28.6.2 the Supplier fails to perform its obligations in accordance with this Agreement, the Authority shall not be entitled to receive Service Credits to the extent that a Performance Failure has been caused by the Force Majeure Event;

28.6.3 the Supplier shall be entitled to receive payment of the Charges (or a proportional payment of them) only to the extent that the Services (or part of the Services) continue to be performed in accordance with the terms of this Agreement during the occurrence of the Force Majeure Event.

28.7 The Affected Party shall notify the other Party as soon as practicable after the Force Majeure Event ceases or no longer causes the Affected Party to be unable to comply with its obligations under this Agreement.

28.8 Relief from liability for the Affected Party under this Clause 28 shall end as soon as the Force Majeure Event no longer causes the Affected Party to be unable to comply with its obligations under this Agreement and shall not be dependent on the serving of notice under Clause 28.7.

SECTION I – TERMINATION AND EXIT MANAGEMENT

29. TERMINATION RIGHTS

Termination by the Authority

29.1 The Authority may terminate this Agreement by issuing a Termination Notice to the Supplier:-

29.1.1 for convenience at any time, including where the Agreement should not have been entered into in view of a serious infringement of obligations under UK Law;

29.1.2 if a Supplier Termination Event occurs;

29.1.3 if a Force Majeure Event endures for a continuous period of more than ninety (90) days; or

29.1.4 if the Agreement has been substantially amended to the extent that the Public Contracts Regulations 2015 require a new procurement procedure,

and this Agreement shall terminate on the date specified in the Termination Notice.

29.2 Where the Authority:-

29.2.1 has the right to terminate this Agreement under Clause 29.1.1 (*Termination by the Authority*), it may, prior to or instead of terminating the whole of this Agreement, serve a Termination Notice requiring the partial termination of this Agreement, including any part of the provision of the Services or the provision of the Services to any Service Recipient; and/or

29.2.2 is terminating this Agreement under Clause 29.1.2 due to the occurrence of either paragraph (b) of the definition of Supplier Termination Event, it may rely on a single material Default or on a number of Defaults or repeated Defaults (whether of the same or different obligations and regardless of whether such Defaults are cured) which taken together constitute a material Default; and/or

29.2.3 has the right to terminate this Agreement under Clause 29.1.2 or Clause 29.1.3, it may, prior to or instead of terminating the whole of this Agreement, serve a Termination Notice requiring the partial termination of this Agreement to the extent that it relates to any part of the Services which are materially affected by the relevant circumstances.

Termination by the Supplier

29.3 The Supplier may, by issuing a Termination Notice to the Authority, terminate this Agreement if the Authority fails to pay an undisputed sum due to the Supplier under this Agreement which in aggregate exceeds the Annual Contract Value for the Term or Extension Period and such amount remains outstanding forty (40) Working Days after the receipt by the Authority of a notice of non-payment from the Supplier. Following such Termination Notice, this Agreement shall then terminate on the date specified in the Termination Notice (which shall not be less than sixty (60) Working Days from the date of the issue of the Termination Notice).

Partial Termination

29.4 The Parties shall agree the effect of any Change necessitated by a Partial Termination in accordance with the Change Control Procedure, including the effect the Partial Termination may have on any other Services and the Charges, provided that:-

29.4.1 the Supplier shall not be entitled to an increase in the Charges in respect of the Services that have not been terminated if the Partial Termination arises due to the occurrence of a Supplier Termination Event;

29.4.2 any adjustment to the Charges (if any) shall be calculated in accordance with the Financial Model and must be reasonable; and

29.4.3 the Supplier shall not be entitled to reject the Change.

30. CONSEQUENCES OF EXPIRY OR TERMINATION

General Provisions on Expiry or Termination

30.1 The provisions of Clauses 5.7 (*Specially Written Software warranty*), 9.4 and 9.5 (VAT), **Error! Reference source not found.** (*Set-off and Withholding*), 11 (*Records, Reports, Audits and Open Book Data*), 13.3 (*Employment Indemnity*), 13.4 (*Income Tax and National Insurance Contributions*), 15 (*Intellectual Property Rights*), 16 (*Licences Granted by the Supplier*), 18.1 (*IPRs Indemnity*), 20 (*Confidentiality*), 21 (*Transparency and Freedom of Information*), 22 (*Protection of Personal Data*), 24 (*Limitations on Liability*), 30 (*Consequences of Expiry or Termination*), 36 (*Severance*), 38 *(Entire Agreement*), 39 (*Third Party Rights*), 41 (*Disputes*) and 42 (*Governing Law and Jurisdiction*), and the provisions of Schedules 1 (*Definitions*), 7.1 (*Charges and Invoicing*), 7.5 (*Financial and Audit Rights*), 8.3 (*Dispute Resolution Procedure*), 8.4 (*Reports and Records Provisions*), 8.5 (*Exit Management*) and 9.1 (*Staff Transfer*), and each Party's accrued rights and liabilities, shall survive the termination or expiry of this Agreement.

Exit Management

30.2 The Parties shall comply with the provisions of Schedule 8.5 (*Exit Management*) and any current Exit Plan in relation to orderly transition of the Services to the Authority or a Replacement Supplier.

Payments by the Authority

30.3 If this Agreement is terminated by the Authority pursuant to Clause 29.1.1 (*Termination by the Authority*) or by the Supplier pursuant to Clause 29.3 (*Termination by the Supplier*), the Authority shall pay the Supplier the sum specified in Clause 24.4.1 (*Financial and other Limits*) (which shall be the Supplier's sole remedy for the termination of this Agreement).

30.4 If this Agreement is terminated (in part or in whole) by the Authority pursuant to Clauses 29.1.1, 29.1.3 and/or 29.2 *(Termination by the Authority*), or the Term expires, the only payments that the Authority shall be required to make as a result of such termination (whether by way of compensation or otherwise) are:-

30.4.1 payments in respect of any Assets or apportionments in accordance with Schedule 8.5 (*Exit Management*); and

30.4.2 payments in respect of unpaid Charges for Services received up until the Termination Date.

30.5 The costs of termination incurred by the Parties shall lie where they fall if:-

30.5.1 the Authority terminates or partially terminates this Agreement for a continuing Force Majeure Event pursuant to Clause 29.1.3 or 29.2.3 (*Termination by the Authority*); or

30.5.2 the Authority terminates this Agreement under Clause 29.1.4.

Payments by the Supplier

In the event of Supplier Termination Event, the Supplier shall repay to the Authority all Charges it has been paid in advance. **SECTION J - MISCELLANEOUS AND GOVERNING LAW**

31. **COMPLIANCE**

Health and Safety

31.1 The Supplier shall perform its obligations under this Agreement (including those in relation to the Services) in accordance with:-

31.1.1 all applicable Law regarding health and safety; and

31.1.2 the Health and Safety Policy whilst at the Authority Premises.

31.2 Each Party shall notify the other as soon as practicable of any health and safety incidents or material health and safety hazards at the Authority Premises of which it becomes aware and which relate to or arise in connection with the performance of this Agreement. The Supplier shall instruct the Supplier Personnel to adopt any necessary associated safety measures in order to manage any such material health and safety hazards.

Equality and Diversity

31.3 The Supplier shall:-

31.3.1 perform its obligations under this Agreement (including those in relation to the Services) in accordance with:-

(a) all applicable equality Law (whether in relation to race, sex, gender reassignment, age, disability, sexual orientation, religion or belief, pregnancy, maternity or otherwise);

(b) the Authority's equality and diversity policy as provided to the Supplier from time to time; and

(c) any other requirements and instructions which the Authority reasonably imposes in connection with any equality obligations imposed on the Authority or Service Recipients at any time under applicable equality Law;

31.3.2 take all necessary steps, and inform the Authority of the steps taken, to prevent unlawful discrimination designated as such by any court or tribunal, or the Equality and Human Rights Commission or (any successor organisation).

Modern Slavery Act 2015

31.4 In performing its obligations under this agreement, the supplier shall:

31.4.1 comply with all applicable anti-slavery and human trafficking laws, statutes, regulations and codes from time to time in force including the Modern Slavery Act 2015;

31.4.2 Have and maintain throughout the term its own policies and procedures to ensure compliance;

31.4.3 not engage in any activity, practice or conduct that would constitute an offence under sections 1, 2 or 4, of the Modern Slavery Act 2015 if such activity, practice or conduct were carried out in the United Kingdom; and

31.4.4 include in its contracts with its sub-contractors and suppliers anti-slavery and human trafficking provisions that are at least as onerous as those set out in this clause 31.4.

31.5 The Supplier represents, warrants and undertakes that neither it nor any of its officers, employees or other persons associated with it:

31.5.1 has been convicted of any offence involving slavery and human trafficking: and

31.5.2 has been or is the subject of any investigation, inquiry or enforcement proceeding by any governmental, administrative or regulatory body regarding any offence or alleged offence of or in connection with slavery and human trafficking

31.6 The supplier shall implement due diligence procedures for its sub-contractors, suppliers and other participants in its supply chains, to ensure that there is no slavery or human trafficking in its supply chains

31.7 Any breach of this clause 31.4 by the supplier shall constitute a material breach of this agreement.

Official Secrets Act and Finance Act

31.8 The Supplier shall comply with the provisions of:-

31.8.1 the Official Secrets Acts 1911 to 1989; and

31.8.2 section 182 of the Finance Act 1989.

32. ASSIGNMENT AND NOVATION

32.1 The Supplier shall not assign, novate or otherwise dispose of or create any trust in relation to any or all of its rights, obligations or liabilities under this Agreement without the prior written consent of the Authority.

32.2 The Authority may at its discretion assign, novate or otherwise dispose of any or all of its rights, obligations and liabilities under this Agreement and/or any associated licences to:-

32.2.1 any Central Government Body; or

32.2.2 to a body other than a Central Government Body (including any private sector body) which performs any of the functions that previously had been performed by the Authority,

and the Supplier shall, at the Authority's request, enter into a novation agreement in such form as the Authority shall reasonably specify in order to enable the Authority to exercise its rights pursuant to this Clause 32.2.

32.3 A change in the legal status of the Authority such that it ceases to be a Central Government Body shall not (subject to Clause 32.4) affect the validity of this Agreement and this Agreement shall be binding on any successor body to the Authority.

32.4 If the Authority assigns, novates or otherwise disposes of any of its rights, obligations or liabilities under this Agreement to a body which is not a Central Government Body or if a body which is not a Central Government Body succeeds the Authority (any such body a "**Successor Body**"), the Supplier shall have the right to terminate for an Insolvency Event affecting the Successor Body identical to the right of termination of the Authority under paragraph (i) of the definition of Supplier Termination Event (as if references in that paragraph (i) to the Supplier and the Guarantor were references to the Successor Body).

33. WAIVER AND CUMULATIVE REMEDIES

33.1 The rights and remedies under this Agreement may be waived only by notice and in a manner that expressly states that a waiver is intended. A failure or delay by a Party in ascertaining or exercising a right or remedy provided under this Agreement or by law shall not constitute a waiver of that right or remedy, nor shall it prevent or restrict the further exercise of that or any other right or remedy.

No single or partial exercise of any right or remedy shall prevent or restrict the further exercise of that or any other right or remedy.

33.2 Unless otherwise provided in this Agreement, rights and remedies under this Agreement are cumulative and do not exclude any rights or remedies provided by law, in equity or otherwise.

34. RELATIONSHIP OF THE PARTIES

34.1 Except as expressly provided otherwise in this Agreement, nothing in this Agreement, nor any actions taken by the Parties pursuant to this Agreement, shall create a partnership, joint venture or relationship of employer and employee or principal and agent between the Parties, or authorise either Party to make representations or enter into any commitments for or on behalf of any other Party.

34.2 Notwithstanding anything to the contrary in this Agreement, the Supplier acknowledges that it is not, and nor will it be, the exclusive supplier of the Services or any other similar goods and services to the Authority and/or the Service Recipients and that the Authority and Service Recipients may perform, or engage a third party to provide any or all of the Services or any similar services.

35. PREVENTION OF FRAUD AND BRIBERY

35.1 The Supplier represents and warrants that neither it, nor to the best of its knowledge any Supplier Personnel, have at any time prior to the Effective Date:-

35.1.1 committed a Prohibited Act or been formally notified that it is subject to an investigation or prosecution which relates to an alleged Prohibited Act; and/or

35.1.2 been listed by any government department or agency as being debarred, suspended, proposed for suspension or debarment, or otherwise ineligible for participation in government procurement programmes or contracts on the grounds of a Prohibited Act.

35.2 The Supplier shall not during the term of this Agreement:-

35.2.1 commit a Prohibited Act; and/or

35.2.2 do or suffer anything to be done which would cause the Authority or any of the Authority's employees, consultants, contractors, sub-contractors or agents to contravene any of the Relevant Requirements or otherwise incur any liability in relation to the Relevant Requirements.

35.3 The Supplier shall during the term of this Agreement:-

35.3.1 establish, maintain and enforce, and require that its Sub-contractors establish, maintain and enforce, policies and procedures which are adequate to ensure compliance with the Relevant Requirements and prevent the occurrence of a Prohibited Act;

35.3.2 have in place reasonable prevention measures (as defined in sections 45(3) and 46(4) of the Criminal Finance Act 2017) to ensure that Associated Persons of the Supplier do not commit tax evasion facilitation offences as defined under that Act;

35.3.3 keep appropriate records of its compliance with its obligations under Clause 35.3.1 and make such records available to the Authority on request; and

35.3.4 take account of any guidance about preventing facilitation of tax evasion offences which may be published and updated in accordance with section 47 of the Criminal Finances Act 2017.

35.4 The Supplier shall immediately notify the Authority in writing if it becomes aware of any breach of Clause 35.1 and/or 35.2, or has reason to believe that it has or any of the Supplier Personnel have:-

35.4.1 been subject to an investigation or prosecution which relates to an alleged Prohibited Act;

35.4.2 been listed by any government department or agency as being debarred, suspended, proposed for suspension or debarment, or otherwise ineligible for participation in government procurement programmes or contracts on the grounds of a Prohibited Act; and/or

35.4.3 received a request or demand for any undue financial or other advantage of any kind in connection with the performance of this Agreement or otherwise suspects that any person or Party directly or indirectly connected with this Agreement has committed or attempted to commit a Prohibited Act.

35.5 If the Supplier makes a notification to the Authority pursuant to Clause 35.4, the Supplier shall respond promptly to the Authority's enquiries, co-operate with any investigation, and allow the Authority to Audit any books, Records and/or any other relevant documentation in accordance with Clause 11 (Records, Reports, Audits and Open Book Data).

35.6 If the Supplier is in Default under Clauses 35.1 and/or 35.2, the Authority may by notice:-

35.6.1 require the Supplier to remove from performance of this Agreement any Supplier Personnel whose acts or omissions have caused the Default; or

35.6.2 immediately terminate this Agreement.

35.7 Any notice served by the Authority under Clause 35.6 shall specify the nature of the Prohibited Act, the identity of the Party who the Authority believes has committed the Prohibited Act and the action that the Authority has elected to take (including, where relevant, the date on which this Agreement shall terminate).

36. SEVERANCE

If any provision of this Agreement (or part of any provision) is held to be void or otherwise unenforceable by any court of competent jurisdiction, such provision (or part) shall to the extent necessary to ensure that the remaining provisions of this Agreement are not void or unenforceable be deemed to be deleted and the validity and/or enforceability of the remaining provisions of this Agreement shall not be affected.

37. FURTHER ASSURANCES

Each Party undertakes at the request of the other, and at the cost of the requesting Party to do all acts and execute all documents which may be reasonably necessary to give effect to the meaning of this Agreement.

38. ENTIRE AGREEMENT

38.1 This Agreement constitutes the entire agreement between the Parties in respect of its subject matter and supersedes and extinguishes all prior negotiations, arrangements, understanding, course of dealings or agreements made between the Parties in relation to its subject matter, whether written or oral.

38.2 Neither Party has been given, nor entered into this Agreement in reliance on, any warranty, statement, promise or representation other than those expressly set out in this Agreement.

38.3 Nothing in this Clause 38 shall exclude any liability in respect of misrepresentations made fraudulently.

39. THIRD PARTY RIGHTS

39.1 The provisions of this Agreement confer benefits on the Service Recipients and, in addition, the provisions of Clause 18.1 (*IPRs Indemnity*), paragraphs 2.1, 2.6, 3.1 and 3.3 of Part C and paragraphs 1.4, 2.3 and 2.8 of Part E of Schedule 9.1 (*Staff Transfer*) and the provisions of paragraph 6.9 of Schedule 8.5 (*Exit Management*) confer benefits on persons named in such provisions other than the Parties (such provisions together being referred to as "**Third Party Provisions**" and each Service Recipient and each such person being referred to as a "**Third Party Beneficiary**"). The Third Party Provisions are intended to be enforceable by Third Parties Beneficiaries by virtue of the CRTPA.

39.2 In respect of any Losses suffered by any or all of the Third Party Beneficiaries in connection with this Agreement:

39.2.1 such Losses shall be deemed to be suffered by the Authority and, to the extent they would be recoverable from the Supplier under this Agreement had they been Losses suffered by the Authority, shall be recoverable by the Authority against the Supplier; and

39.2.2 the exercise of any right or the commencement of civil proceedings shall be brought solely by the Authority unless it is expressly prevented by a first instance decision of the English courts from exercising a right or commencing civil proceedings in respect of any Losses or right of action on behalf of the relevant Third Party Beneficiary on the basis that the Authority is not an interested party.

39.3 Subject to Clauses 39.1 and 39.2, a person who is not a Party to this Agreement has no right under the CRTPA to enforce any term of this Agreement but this does not affect any right or remedy of any person which exists or is available otherwise than pursuant to that Act.

39.4 Any amendments or modifications to this Agreement may be made, and any rights created under Clause 39.1, may be altered or extinguished by the Parties without the consent of any Third Party Beneficiary.

40. NOTICES

40.1 Any notices sent under this Agreement must be in writing.

40.2 Subject to Clause 40.4, the following table sets out the method by which notices may be served under this Agreement and the respective deemed time and proof of service:-

Manner of Delivery	Deemed time of service	Proof of service
Email	9.00am on the first Working Day after sending	Dispatched as a pdf attachment to an e-mail to the correct e-mail address without any error message
Personal delivery	On delivery, provided that delivery is between 9.00am and 5.00pm on a Working Day. Otherwise, delivery will occur at 9.00am on the next Working Day	Properly addressed and delivered as evidenced by signature of a delivery receipt
Prepaid, Royal Mail Signed For™ 1st Class or other prepaid, next working day service providing proof of delivery	At the time recorded by the delivery service, provided that delivery is between 9.00am and 5.00pm on a Working Day. Otherwise, delivery will occur at 9.00am on the same Working Day (if delivery before	Properly addressed prepaid and delivered as evidenced by signature of a delivery receipt

	9.00am) or on the next Working Day (if after 5.00pm)	

40.3 Notices shall be sent to the addresses set out below or at such other address as the relevant Party may give notice to the other Party for the purpose of service of notices under this Agreement:-

	Supplier	**Authority**
Contact	[Legal General]	**[Redacted For Publishing]**
Address	Resilinc 1525 McCarthy Blvd STE 1122 Milpitas, CA 95035 USA	[Nuclear Decommissioning Authority, Hinton House, Birchwood Park Avenue, Risley, Warrington WA3 6GR.
Email	legageneral@resilinc.com	**[Redacted For Publishing]**

40.4 The following notices may only be served as an attachment to an email if the original notice is then sent to the recipient by personal delivery or recorded delivery in the manner set out in the table in Clause 40.2:-

40.4.1 Force Majeure Notices;

40.4.2 notices issued by the Supplier pursuant to Clause 29.3 *(Termination by the Supplier*);

40.4.3 Termination Notices; and

40.4.4 Dispute Notices.

40.5 Failure to send any original notice by personal delivery or recorded delivery in accordance with Clause 40.4 shall invalidate the service of the related e-mail transmission. The deemed time of delivery of such notice shall be the deemed time of delivery of the original notice sent by personal delivery or Royal Mail Signed For™ 1st Class delivery (as set out in the table in Clause 40.2) or, if earlier, the time of response or acknowledgement by the other Party to the email attaching the notice.

40.6 This Clause 40 does not apply to the service of any proceedings or other documents in any legal action or, where applicable, other method of dispute resolution (other than the service of a Dispute Notice under Schedule 8.3 (*Dispute Resolution Procedure*)).

41. DISPUTES

41.1 The Parties shall resolve Disputes arising out of or in connection with this Agreement in accordance with the Dispute Resolution Procedure.

41.2 The Supplier shall continue to provide the Services in accordance with the terms of this Agreement until a Dispute has been resolved.

42. GOVERNING LAW AND JURISDICTION

42.1 This Agreement and any issues, disputes or claims (whether contractual or non-contractual) arising out of or in connection with it or its subject matter or formation shall be governed by and construed in accordance with the laws of England and Wales.

42.2 Subject to Clause 41 (*Disputes*) and Schedule 8.3 (*Dispute Resolution Procedure*), the Parties agree that the courts of England and Wales shall have exclusive jurisdiction to settle any dispute or claim (whether contractual or non-contractual) that arises out of or in connection with this Agreement or its subject matter or formation.

43. COUNTERPARTS/DUPLICATES

43.1 This Agreement may be executed in any number of counterparts, each of which shall constitute an original, but which shall together constitute one agreement.

43.2 This Agreement may be executed in duplicate, each of which shall constitute an original.

IN WITNESS of which this Agreement has been duly executed by the Parties on the date which appears at the head of its page 1.

Signed for and on behalf of the **NUCLEAR DECOMMISSIONING AUTHORITY**:	**[Redacted For Publishing]**
Signed for and on behalf of RESILINC CORPORATION	**[Redacted For Publishing]**

LIST OF SCHEDULES

SCHEDULE 1

Definitions

Unless otherwise provided or the context otherwise requires the following expressions shall have the meanings set out below.

"**Accounting Reference Date**"	means the dates to which the Supplier prepares its audited financial statements;
"**Accreditation**"	means the assessment of the Core Information Management System in accordance with paragraph 6 of Schedule 2.4 (*Security Management*) by the Authority or an independent information risk manager/professional appointed by the Authority, which results in an Accreditation Decision;
"**Accreditation Decision**"	means the decision of the Authority, taken in accordance with the process set out in paragraph 6 Schedule 2.4 (*Security Management*), to issue the Supplier with a Risk Management Approval Statement or a Risk Management Rejection Notice in respect of the Core Information Management System;
"**Accreditation Plan**"	means the Supplier's plan to attain an Accreditation Approval Statement from the Authority, which is prepared by the Supplier and approved by the Authority in accordance with paragraph 5.4 of Schedule 2.4 (*Security Management*)
"**Achieve**"	means in respect of a Milestone, that the Milestone has been achieved and the relevant component items (including Deliverables) and activities comprised within the Milestone have been performed and a Milestone Achievement Certificate in respect of that Milestone has been issued in accordance with the provisions of Schedule 6.2 (*Milestone Achievement Procedure*), and "**Achieved**" and "**Achievement**" shall be construed accordingly;
"Achievement Criteria"	means, in respect of any Milestone, the relevant criteria specified in this Agreement or, where no criteria are so specified, the criteria agreed by the Parties including in the Implementation Plan or a Change Authorisation Note (as applicable)
"Additional Development"	means any unforeseen development tasks or projects post System implementation e.g. the implementation of an additional Application Programming Interface to an external government database.
"**Additional Milestone**"	means a Milestone which is additional to the Milestones set out in the Implementation Plan and will apply to the provision of Services as part of a Project or in connection with the Change Control Procedure;
"Additional Services"	mean any ad hoc requirements post System implementation e.g. changes to System branding or additional Authority training post System implementation.
"**Affected Party**"	means the Party seeking to claim relief in respect of a Force Majeure Event;
"**Affiliate**"	means in relation to a body corporate, any other entity which directly or indirectly Controls, is Controlled by, or is under direct or indirect common Control with, that body corporate from time to time;
"Annual Contract Value"	means the Contract Award Value for the Term or Extension Period of the Agreement divided by the duration of that respective Term or Extension

Period, e.g. the Annual Contract Value for an agreement with a four (4) year Term and Contract Award Value of £100,000 is equal to £25,000.

"**Annual Revenue**" means, for the purposes of determining whether an entity is a Public Sector Dependent Supplier, the audited consolidated aggregate revenue (including share of revenue of joint ventures and Associates) reported by the Supplier or, as appropriate, the Supplier Group in its most recent published accounts, subject to the following methodology:-

(a) figures for accounting periods of other than twelve (12) months should be scaled pro rata to produce a proforma figure for a twelve (12) month period; and

(b) where the Supplier, the Supplier Group and/or their joint ventures and Associates report in a foreign currency, revenue should be converted to British Pound Sterling at the closing exchange rate on the Accounting Reference Date;

"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 Authority 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 Authority
   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.

"Application Programming Interface" or "**API**" means a piece of software that facilitates access to the Supplier's application(s) to provide access to business functionality and/or Authority Data to support any relevant Termination Services which conforms to the Government Digital Service API technical and data standards set online at:

https://www.gov.uk/guidance/gdsapitechnicalanddatastandards

"Acquired Rights Directive" means the European Council Directive 77/187/EEC on the approximation of laws of European member states relating to the safeguarding of employees'

	rights in the event of transfers of undertakings, businesses or parts of undertakings or businesses, as amended or re-enacted from time to time;
"**Assets**"	means all assets and rights used by the Supplier to provide the Services in accordance with this Agreement but excluding the Authority Assets;
"**Associated Person**"	has the meaning given to it in section 44(4) of the Criminal Finances Act 2017;
"**Associates**"	means, in relation to an entity, an undertaking in which the entity owns, directly or indirectly, between 20% and 50% of the voting rights and exercises a degree of control sufficient for the undertaking to be treated as an associate under generally accepted accounting principles;
"**Assurance**"	means written confirmation from a Relevant Authority to the Supplier that the CRP Information is approved by the Relevant Authority;
"**Audit**"	means any exercise by the Authority of its Audit Rights pursuant to Clause 11 (*Records, Reports, Audit and Open Book Data*) and Schedule 7.5 (*Financial Reports and Audit Rights*);
"**Audit Agents**"	means:-
	(a) the Authority's internal and external auditors;
	(b) the Authority's statutory or regulatory auditors;
	(c) the Comptroller and Auditor General, their staff and/or any appointed representatives of the National Audit Office;
	(d) HM Treasury or the Cabinet Office;
	(e) any party formally appointed by the Authority to carry out audit or similar review functions;
	(f) a Service Recipient or any person falling within the scope of Paragraphs (a), (b) or (e) with respect to the Service Recipient; and
	(g) successors or assigns of any of the above;
"**Audit Rights**"	means the audit and access rights referred to in Schedule 7.5 (*Financial Reports and Audit Rights*);
"**Authority Assets**"	means the Authority Materials, the Authority's or Service Recipient's infrastructure and any other data, software, assets, equipment or other property owned by and/or licensed or leased to the Authority or any Service Recipient and which is or may be used in connection with the provision or receipt of the Services;
"**Authority Background IPRs**"	means:-
	(a) IPRs owned by the Authority or a Service Recipient before the Effective Date, including IPRs contained in any of the Authority's or Service Recipient's knowhow, documentation, processes and procedures;
	(b) IPRs created by the Authority or a Service Recipient independently of this Agreement; and/or

(c) Crown Copyright which is not available to the Supplier otherwise than under this Agreement;

"**Authority Cause**" means any material breach by the Authority of any of the Authority Responsibilities, except to the extent that such breach is:-

(a) the result of any act or omission by the Authority to which the Supplier has given its prior consent; or

(b) caused by the Supplier, any Sub-contractor or any Supplier Personnel;

"**Authority Change Manager**" means the person appointed to that position by the Authority from time to time and notified in writing to the Supplier or, if no person is notified, the Authority Representative;

"**Authority Data**" means:-

(a) the data, text, drawings, diagrams, images or sounds (together with any database made up of any of these) which are embodied in any electronic, magnetic, optical or tangible media, and which are:-

(i) supplied to the Supplier by or on behalf of the Authority or a Service Recipient; and

(ii) which the Supplier is required to generate, process, store or transmit pursuant to this Agreement; or

(b) any Personal Data for which the Authority or a Service Recipient is the Data Controller;

"**Authority Materials**" means the Authority Data together with any materials, documentation, information, programs and codes supplied by the Authority or a Service Recipient to the Supplier, the IPRs in which:-

(a) are owned or used by or on behalf of the Authority or a Service Recipient; and

(b) are or may be used in connection with the provision or receipt of the Services,

but excluding any Licensed Software;

"**Authority Personal Data**" means the Authority Data that constitutes Personal Data (such being anticipated to fall within the scope of the description set out in the Appendix to the Supplier Solution) where such Personal Data is Processed by either Party under this Agreement;

"**Authority Premises**" means premises owned, controlled or occupied by the Authority, a Service Recipient and/or any Central Government Body which are made available for use by the Supplier or its Sub-contractors for provision of the Services (or any of them);

"**Authority Representative**" means the representative appointed by the Authority pursuant to Clause 10.2 (*Representatives*), as notified to the Authority from time to time;

"**Authority Requirements**" means the requirements of the Authority set out in Schedules *2.1 (Services Description), 2.2 (Performance Levels), 2.3 (Standards), 2.4 (Security Management), 2.5 (Insurance Requirements), 6.1 (Implementation Plan), 8.4 (Reports and Records Provisions), 8.5 (Exit Management) and*

	8.6 (Service Continuity Plan) and those set out in a Change Authorisation Note for a Project;
"**Authority Responsibilities**"	means the responsibilities of the Authority specified in Schedule 3 (*Authority Responsibilities*);
"**Authority System**"	means the Authority's and Service Recipients' computing environment (consisting of hardware, software and/or telecommunications networks or equipment) used by the Authority, a Service Recipient or the Supplier in connection with this Agreement which is owned by the Authority or a Service Recipient or licensed to either of them by a third party and which interfaces with the Supplier System or which is necessary for the Authority and/or Service Recipients to receive the Services;
"**Available**"	has the meaning given in paragraph 1.2 of Part 2 of Appendix 1 in Schedule 2.2 *(Performance Levels)*
"**Baseline Security Requirements**"	means the Authority's baseline security requirements, the current copy of which is contained in Appendix 1 of Schedule 2.4 (*Security Management*), as updated from time to time by the Authority and notified to the Supplier;
"Beneficiary"	has the meaning given in paragraph 1.1 of Schedule 8.7 (*Conduct of Claims*);
"**Boards**"	means the Joint Implementation Board, or Commercial Systems Governance Board.
"**Board Member**"	means the initial persons appointed by the Authority and Supplier to the Boards or Forums as set out in Appendix 1 of Schedule 8.1 (*Governance*) and any replacements from time to time agreed by the Parties in accordance with paragraph 3.3 of Schedule 8.1 (*Governance*);
"**Breach of Security**"	means the occurrence of:- a. any unauthorised access to or use of the Services, the Authority Premises, the Sites, the Supplier System, the Authority System and/or any information or data (including the Confidential Information and the Authority Data) used by the Authority, the Supplier or any Subcontractor in connection with this Agreement; b. the loss (physical or otherwise) and/or unauthorised disclosure of any information or data (including the Confidential Information and the Authority Data), including copies of such information or data, used by the Authority, the Supplier or any Subcontractor in connection with this Agreement; and/or c. any part of the Supplier System ceasing to be compliant with the Certification Requirements, in each case as more particularly set out in the security requirements in Schedule 2.1 (*Services Description*) and the Baseline Security Requirements;
"**Breakage Costs Payment**"	an amount equal to the Contract Breakage Costs as at the Termination Date as determined in accordance with paragraph 3 of Schedule 7.2 (Payments on Termination);
"**Business Continuity Plan**"	has the meaning given in paragraph 1.2.1(b) of Schedule 8.6 (*Service Continuity Plan*);

"**Business Continuity Services**"	has the meaning given in paragraph 3.2.2 of Schedule 8.6 (*Service Continuity Plan*);
"**Cabinet Office Markets and Suppliers Team**"	means the UK government's team responsible for managing the relationship between government and its Strategic Suppliers, or any replacement or successor body carrying out the same function;
"Call Answering Time"	means the time taken for a Help Desk operative to answer a voice call, i.e. not a voicemail automatic answering service
"CaSIE"	means government's Contracts and Spend Insight Engine online tool, developed on the Microsoft Power BI application to analyse contract and spend data across the public sector.
"**CEDR**"	the Centre for Effective Dispute Resolution of International Dispute Resolution Centre, 70 Fleet Street, London, EC4Y 1EU.
"**Central Government Body**"	means a body listed in one of the following sub-categories of the Central Government classification of the Public Sector Classification Guide, as published and amended from time to time by the Office for National Statistics:- (a) Government Department; (b) Non-Departmental Public Body or Assembly Sponsored Public Body (advisory, executive, or tribunal); (c) Non-Ministerial Department; or (d) Executive Agency;
"**Certification Requirements**"	means the requirements set out in paragraph 7 of Schedule 2.4 (*Security Management*);
"**Change**"	means each:- (a) Contract Change; (b) Document Change; and (c) Operational Change;
"**Change Authorisation Note**"	means a form setting out an agreed Contract Change which shall be substantially in the form of Appendix 2 of Schedule 8.2 (*Change Control Procedure*);
"Change Communication"	means any Change Request, Impact Assessment, Change Authorisation Note or other communication sent or required to be sent pursuant to Schedule 8.2 (*Change Control Procedure*);
"**Change Control Procedure**"	means the procedure for changing this Agreement and commissioning Projects as set out in Schedule 8.2 (*Change Control Procedure*);
"**Change in Law**"	means any change in Law which impacts on the performance of the Services which comes into force after the Effective Date;
"**Change Request**"	means a written request for a Contract Change substantially in the form of Appendix 1 of Schedule 8.2 (*Change Control Procedure*);

"Chargeable Change"	has the meaning given to it in paragraph 2.3.1 of Schedule 8.2 (*Change Control Procedure*)
"**Charges**"	means the charges for the provision of the Services set out in or otherwise calculated in accordance with Schedule 7.1 (*Charges and Invoicing*), including any Milestone Payment or Service Charge;
"**Claim**"	has the meaning given in Paragraph 1.2 of Schedule 8.7 (Conduct of Claim)
"**Class 1 Transaction**"	has the meaning set out in the listing rules issued by the UK Listing Authority;
"**CNI**"	means Critical National Infrastructure;
"Commercial Sensitive Information"	means the information listed in Schedule 4.2 (Commercially Sensitive Information) comprising the information of a commercially sensitive nature relating to:- (a) the pricing of the Services; (b) the details of the Supplier's IPRs; and (c) the Supplier's business and investment plans which the Supplier has indicated to the Authority that, if disclosed by the Authority, would cause the Supplier significant commercial disadvantage or material financial loss.
"Commercial Systems Governance Board"	means the body described in paragraph 5 of Schedule 8.1 (*Governance*)
"**Comparable Supply**"	means the supply of services to another customer of the Supplier that are the same or similar to any of the Services;
"**Confidential Information**"	means:- (a) Information, including all Personal Data, which (however it is conveyed) is provided by the Disclosing Party pursuant to or in anticipation of this Agreement that relates to:- (i) the Disclosing Party Group; or (ii) the operations, business, affairs, developments, intellectual property rights, trade secrets, knowhow and/or personnel of the Disclosing Party Group; (b) other Information provided by the Disclosing Party pursuant to or in anticipation of this Agreement that is clearly designated as being confidential or equivalent or that ought reasonably to be considered to be confidential (whether or not it is so marked) which comes (or has come) to the Recipient's attention or into the Recipient's possession in connection with this Agreement; (c) discussions, negotiations, and correspondence between the Disclosing Party or any of its directors, officers, employees, consultants or professional advisers and the Recipient or any of its directors, officers, employees, consultants and professional advisers in connection with this Agreement and all matters arising therefrom; and

(d) Information derived from any of the above,

but not including any Information which:-

(i) was in the possession of the Recipient without obligation of confidentiality prior to its disclosure by the Disclosing Party;

(ii) the Recipient obtained on a nonconfidential basis from a third party who is not, to the Recipient's knowledge or belief, bound by a confidentiality agreement with the Disclosing Party or otherwise prohibited from disclosing the information to the Recipient;

(iii) 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;

(iv) was independently developed without access to the Confidential Information; or

(v) relates to the Supplier's:-

(1) performance under this Agreement; or

(2) failure to pay any Subcontractor as required pursuant to Clause 14.5.1 (*Supply Chain Protection*);

"Contract Award Value" the monetary value of the contract awarded for the Term (or Extended Term should the option to extend be invoked) as at the time of contract award. The value of the Term is **£1,550,640.00**;

"**Contract Change**" means any change to this Agreement, including a Project, other than an Operational Change or Document Change;

"Contracts and Spend Insight Engine" means government's online tool, developed on the Microsoft Power BI application to analyse contract and spend data across the public sector;

"**Contact Data**" means the Personal Data of each Party's Employees Processed by the other Party, under, or in connection with, this Agreement;

"**Contract Breakage Costs**" the amounts payable by the Supplier to its Key Subcontractors or other third parties (as applicable) for terminating all relevant Key Subcontracts or Third Party Contracts as a direct result of the early termination of this Agreement;

"**Contract Change**" means any change to this Agreement, including commissioning a Project, other than an Operational Change or Document Change;

"**Contract Year**" means:-

(a) a period of twelve (12) months commencing on the Effective Date; or

(b) thereafter a period of twelve (12) months commencing on each anniversary of the Effective Date,

provided that the final Contract Year shall end on the expiry or termination of the Term;

"**Control**"	means the possession by person, directly or indirectly, of the power to direct or cause the direction of the management and policies of the other person (whether through the ownership of voting shares, by contract or otherwise) and "**Controls**" and "**Controlled**" shall be interpreted accordingly;
"Controlled Document"	means a document on the List of Controlled Documents as set out in Appendix 3 of Schedule 8.2 (*Change Control Procedure*);
"**Controller**"	has the meaning given in the Data Protection Legislation;
"**Core Information Management System**"	means those information assets, ICT systems and/or Sites which will be used by the Supplier and/or its Subcontractors to Process Authority Data, together with the associated information management system (including organisational structure, controls, policies, practices, procedures, processes and resources), which the Authority has determined in accordance with paragraph 5 of Schedule 2.4 (*Security Management*) shall be subject to Accreditation;
"**Corporate Change Event**"	means:-

(a) any change of Control of the Supplier or a Parent Undertaking of the Supplier;

(b) any change of Control of any member of the Supplier Group which, in the reasonable opinion of the Authority, could have a material adverse effect on the Services;

(c) any change to the business of the Supplier or any member of the Supplier Group which, in the reasonable opinion of the Authority, could have a material adverse effect on the Services;

(d) a Class 1 Transaction taking place in relation to the shares of the Supplier or any Parent Undertaking of the Supplier whose shares are listed on the main market of the London Stock Exchange plc;

(e) an event that could reasonably be regarded as being equivalent to a Class 1 Transaction taking place in respect of the Supplier or any Parent Undertaking of the Supplier;

(f) payment of dividends by the Supplier or the ultimate Parent Undertaking of the Supplier Group exceeding 25% of the net asset value of the Supplier or the ultimate Parent Undertaking of the Supplier Group respectively in any twelve (12) month period;

(g) an order is made or an effective resolution is passed for the winding up of any member of the Supplier Group;

(h) any member of the Supplier Group stopping payment of its debts generally or becoming unable to pay its debts within the meaning of section 123(1) of the Insolvency Act 1986 or any member of the Supplier Group ceasing to carry on all or substantially all its business, or any compromise, composition, arrangement or agreement being made with creditors of any member of the Supplier Group;

(i) the appointment of a receiver, administrative receiver or administrator in respect of or over all or a material part of the undertaking or assets of any member of the Supplier Group; and/or

(j) any process or events with an effect analogous to those in paragraphs (e) to (g) inclusive above occurring to a member of the Supplier Group in a jurisdiction outside England and Wales;

"**Corporate Resolution Planning Information**" means, together, the:-

(a) Group Structure Information and Resolution Commentary; and

(b) UK Public Sector and CNI Contract Information;

"**Costs**" means the following costs (without double recovery) to the extent that they are reasonably and properly incurred by the Supplier or, as applicable, a Key Sub-contractor in providing the Services:-

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

(i) base salary paid to the Supplier Personnel

(ii) employer's national insurance contributions

(iii) car allowances

(iv) any other contractual employment benefits

(v) work place IT equipment and tools reasonably necessary to provide the Services (but not including items included within paragraph (b) below) and

(vi) reasonable recruitment costs, as agreed with the Authority

(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 Authority or (to the extent that risk and title in any Asset is not held by the Supplier or relevant Key Sub-contractor) 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 or relevant Key Sub-contractor 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:-

(f) Overhead

(g) financing or similar costs

(h) 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

(i) taxation

(j) fines and penalties and

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

"**COTS**" means Software (including open source software) and/or IPRs that:

(a) the relevant supplier (which may include the Supplier) makes generally available commercially (whether by way of sale, lease or licence) on standard terms which are not typically negotiated by the supplier save as to price and has a Non-trivial Customer Base; or

(b) in respect of Software, is otherwise classified in Schedule 5 (*Software*) as COTS for the purposes of this Agreement, regardless of whether such Software satisfies paragraph (a);

"Credit Rating Threshold" means the minimum failure score of 60 or equivalent for the Supplier of as reported by Dun and Bradstreet Limited (or equivalent financial risk company as may be updated from time to time);

"**Critical National Infrastructure**" means those critical elements of UK national infrastructure (namely assets, facilities, systems, networks or processes and the essential workers that operate and facilitate them), the loss or compromise of which could result in:-

(a) major detrimental impact on the availability, integrity or delivery of essential services – including those services whose integrity, if compromised, could result in significant loss of life or casualties – taking into account significant economic or social impacts; and/or

(b) significant impact on national security, national defence, or the functioning of the UK;

"**Critical Performance Failure**" means the Supplier accruing in aggregate twenty (20) or more Service Points (in terms of the number of points allocated) in any period of three (3) months.

"**Critical Service Contract**" means the overall status of this Agreement as determined by the Authority and specified in paragraph 1.1 of Part 2 to Schedule 8.6 (*Service Continuity Plan*)

"**Crown Copyright**" has the meaning given in the Copyright, Designs and Patents Act 1988;

"**CRP Information**" means the Corporate Resolution Planning Information;

"**CRTPA**" means the Contracts (Rights of Third Parties) Act 1999;

"**Data Handover Period**" means a period commencing on the date on which the this Agreement terminates or expires and ending on the later of (a) six (6) months following such termination or expiry date and (b) the date on which the Authority Data has been fully transferred to the Authority, the relevant Service Recipient or a Replacement Supplier;

"**Data Protection Legislation**"	means any law, statute, declaration, decree, directive, legislative enactment, order, ordinance, regulation, rule or other binding restriction as updated and amended from time to time which relates to the protection of individuals with regards to the processing of Personal Data to which a Party is subject, including the Data Protection Act 2018 and the Privacy and Electronic Communications (EC Directive) Regulations 2003 and the "EU GDPR" and the "UK GDPR", any code of practice or guidance published by the Information Commissioner or other regulator and/or, the European Data Protection Board.
"**Data Subject**"	has the meaning given in the Data Protection Legislation;
"**Data Subject Request**"	means a request or notice from a Data Subject exercising his or her rights under the Data Protection Legislation in relation to the Authority Personal Data;
"**Dedicated Supplier Personnel**"	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 Authority 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
"**Deductions**"	means all Service Credits or any other deduction which is paid or payable to the Authority under this Agreement;
"**Default**"	means any breach of the obligations of the relevant Party (including abandonment of this Agreement in breach of its terms, repudiatory breach or breach of a fundamental term) or any other default, act, omission, negligence or statement:- (a) in the case of the Authority, of its employees, servants, agents; or (b) in the case of the Supplier, of its Subcontractors or any Supplier Personnel, in connection with or in relation to the subject matter of this Agreement and in respect of which such Party is liable to the other;
"**Defect**"	means:- (a) any error, damage or defect in the manufacturing of a Deliverable; or (b) any error or failure of code within the Software which causes a Deliverable to malfunction or to produce unintelligible or incorrect results; or (c) any failure of any Deliverable to provide the performance, features and functionality specified in the Authority Requirements or the Documentation (including any adverse effect on response times) regardless of whether or not it prevents the relevant Deliverable from meeting its associated Test Success Criteria; or (d) any failure of any Deliverable to operate in conjunction with or interface with any other Deliverable in order to provide the performance, features and functionality specified in the Authority Requirements or the Documentation (including any adverse effect on response times) regardless of whether or not it prevents the

relevant Deliverable from meeting its associated Test Success Criteria;

"**Delay**"	means:-
	(a) a delay in the Achievement of a Milestone by its Milestone Date; or
	(b) a delay in the design, development, testing or implementation of a Deliverable by the relevant date set out in the Implementation Plan;
"**Deliverable**"	means an item or feature delivered or to be delivered by the Supplier at or before a Milestone Date or at any other stage during the performance of this Agreement;
"**Detailed Implementation Plan**"	means the plan developed and revised from time to time in accordance with paragraphs 3 and 4 of Schedule 6.1 (*Implementation Plan*);
"**Dependent Parent Undertaking**"	means any Parent Undertaking which provides any of its Subsidiary Undertakings and/or Associates, whether directly or indirectly, with any financial, trading, managerial or other assistance of whatever nature, without which the Supplier would be unable to continue the day to day conduct and operation of its business in the same manner as carried on at the time of entering into this Agreement, including for the avoidance of doubt the provision of the Services in accordance with the terms of this Agreement;
"Development Charges"	mean charges for Additional Development;
"**Disaster**"	means the occurrence of one or more events which, either separately or cumulatively, mean that the Services, or a material part of the Services will be unavailable for a period of twenty-four (24) hours or which is reasonably anticipated will mean that the Services or a material part of the Services will be unavailable for that period;
"**Disaster Recovery Plan**"	has the meaning given in paragraph 1.2.1(c) of Schedule 8.6 (*Service Continuity Plan)*;
"**Disaster Recovery Services**"	means the services embodied in the processes and procedures for restoring the Services following the occurrence of a Disaster;
"**Disaster Recovery System**"	mean the system identified by the Supplier in the Supplier Solution which shall be used for the purpose of delivering the Disaster Recovery Services;
"**Disclosing Party**"	has the meaning given in Clause 20.1 (*Confidentiality*);
"**Disclosing Party Group**"	means:-
	(a) where the Disclosing Party is the Supplier, the Supplier and any Affiliates of the Supplier; and
	(b) where the Disclosing Party is the Authority or a Service Recipient, the Authority, the Service Recipient and any Central Government Body with which the Authority, Service Recipient or the Supplier interacts in connection with this Agreement;
"**Dispute**"	means any dispute, difference or question of interpretation arising out of or in connection with this Agreement, including any dispute, difference or question of interpretation relating to the Services, failure to agree in accordance with the Change Control Procedure or any matter where this Agreement directs

	the Parties to resolve an issue by reference to the Dispute Resolution Procedure;
"**Dispute Notice**"	means a written notice served by one Party on the other stating that the Party serving the notice believes that there is a Dispute;
"**Dispute Resolution Procedure**"	means the dispute resolution procedure set out in Schedule 8.3 (*Dispute Resolution Procedure*);
"Document Change"	means a change to any Controlled Document;
"Document Change Procedure"	means the procedure by which either Party can propose a Document Change in accordance with Schedule 8.2 (*Change Control Procedure*);
"**Documentation**"	means descriptions of the Services and Key Performance Indicators, details of the Supplier System (including (i) vendors and versions for off-the-shelf- components and (configuration details, test scripts, user manuals, operating manuals, process definitions and procedures, and all such other documentation as:- (a) is required to be supplied by the Supplier to the Authority under this Agreement; (b) would reasonably be required by a competent third party capable of Good Industry Practice contracted by the Authority to configure, deploy, run, maintain, upgrade and test the individual systems that provide Services; (c) is required by the Supplier in order to provide the Services; and/or (d) has been or shall be generated for the purpose of providing the Services;
"**DOTAS**"	means the Disclosure of Tax Avoidance Schemes rules which require a promoter of tax schemes to tell HMRC of any specified notifiable arrangements or proposals and to provide prescribed information on those arrangements or proposals within set time limits as contained in Part 7 of the Finance Act 2004 and in secondary legislation made under vires contained in Part 7 of the Finance Act 2004 and as extended to national insurance contributions by the National Insurance Contributions (Application of Part 7 of the Finance Act 2004) Regulations 2012, SI 2012/1868) made under section 132A of the Social Security Administration Act 1992;
"**DPA**"	means the Data Protection Act 2018;
"**Due Diligence Information**"	means any information supplied to the Supplier by or on behalf of the Authority or a Service Recipient prior to the Effective Date;
"**Effective Date**"	means the date on which this Agreement is signed by both Parties;
"**EIRs**"	means the Environmental Information Regulations 2004, together with any guidance and/or codes of practice issued by the Information Commissioner or any Central Government Body in relation to such Regulations;
"**Emergency Exit**"	any termination of this Agreement which is a:- (a) termination of the whole or part of this Agreement in accordance with Clause 29 (*Termination Rights*), except where the period of

notice given under that Clause is greater than or equal to six (6) months

(b) termination of the provision of the Services for any reason prior to the expiry of any period of notice of termination served pursuant to Clause 29 (*Termination Rights*) or

(c) wrongful termination or repudiation of this Agreement by either Party;

"**Employee Liabilities**" means all claims, actions, proceedings, orders, demands, complaints, investigations (save for any claims for personal injury which are covered by insurance) and any award, compensation, damages, tribunal awards, fine, loss, order, penalty, disbursement, payment made by way of settlement and costs, expenses and legal costs reasonably incurred in connection with a claim or investigation related to employment including in relation to the following:-

(a) redundancy payments including contractual or enhanced redundancy costs, termination costs and notice payments;

(b) unfair, wrongful or constructive dismissal compensation;

(c) compensation for discrimination on grounds of sex, race, disability, age, religion or belief, gender reassignment, marriage or civil partnership, pregnancy and maternity or sexual orientation or claims for equal pay;

(d) compensation for less favourable treatment of part-time workers or fixed term employees;

(e) outstanding employment debts and unlawful deduction of wages including any PAYE and national insurance contributions;

(f) employment claims whether in tort, contract or statute or otherwise;

(g) any investigation relating to employment matters by the Equality and Human Rights Commission or other enforcement, regulatory or supervisory body and of implementing any requirements which may arise from such investigation;

"**Employees**" means all staff, including directors, officers and employees, as well as the agents and workers of either Party together with the directors, officers and employees of such Party's sub-contractors or suppliers and further down any contractual chain;

"**Employment Regulations**" means the Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) as amended or replaced or any other Regulations implementing the Acquired Rights Directive the estimated Charges payable by the Authority;

"**End User**" means any person authorised by the Authority to use the IT Environment and/or the Services

"ERP" means Enterprise Resource Planning system.

"EU **GDPR**" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to

	the processing of Personal Data and repealing Directive 95/46/EC (General Data Protection Regulation) OJ L 119/1, 4.5.2016;
"**European Standard**"	means in relation to an electronic invoice means the European standard and any of the syntaxes published in Commission Implementing Decision (EU) 2017/1870.
"EventWatch" API	means the REST application programming interface that provides access to the Resilinc solution through a programmatic interface and is used to integrate event data into third party systems.
"**Exclusive Assets**"	those Assets used by the Supplier or a subcontractor which are used exclusively in the provision of the Services;
"**Exit Day**"	shall have the meaning in the European Union (Withdrawal) Act 2018;
"**Exit Information**"	has the meaning given in paragraph 3.1 of Schedule 8.5 (*Exit Management);*
"**Exit Management**"	means services, activities, processes and procedures to ensure a smooth and orderly transition of all or part of the Services from the Supplier to the Authority and/or a Replacement Supplier, as set out or referred to in Schedule 8.5 (*Exit Management*);
"**Exit Manager**"	the person appointed by each Party pursuant to paragraph 2.3 of Schedule 8.5 (*Exit Management)* for managing the Parties' respective obligations;
"**Exit Plan**"	means the plan produced and updated by the Supplier during the Term in accordance with paragraph 4 of Schedule 8.5 (*Exit Management*);
"**Expedited Dispute Timetable**"	means the reduced timetable for the resolution of Disputes set out in paragraph 3 of Schedule 8.3 (*Dispute Resolution Procedure*);
"**Expert**"	in relation to a Dispute, a person appointed in accordance with paragraph 6.2 of Schedule 8.3 (*Dispute Resolution Procedure*) to act as an expert in relation to that Dispute.
"**Expert Determination**"	determination by an Expert in accordance with paragraph 6 of Schedule 8.3 (*Dispute Resolution Procedure*);
"**Extended Term**"	means the Initial Term as extended by the First Extension Period;
"**Extension Period**"	means the First Extension Period and/or the Second Extension Period;
"**Financial Distress Event**"	means the occurrence of one or more of the events listed in Clause **Error! Reference source not found.** (*Financial Reporting and Assurance*);
"**Fasttrack Change**"	means any Contract Change which the Parties agree to expedite in accordance with paragraph 7 of Schedule 8.2 (*Change Control Procedure*);
"**Financial Transparency Objectives**"	has the meaning given in Paragraph 2 of Schedule 7.5 (*Financial Reports and Audit Rights*);
"Find a Tender Service"	means the platform used to advertise high-value procurement notices. Find a Tender Service ("FTS") replaced the Official Journal of the European Union (OJEU) as the platform for advertising high-value notices on 1st January 2020 following the UK's exit from the EU;
"**First Extension Period**"	means a period of twenty-four (24) months from the end of the Initial Term;

"**FOIA**"	means the Freedom of Information Act 2000 and any subordinate legislation made under that Act from time to time, together with any guidance and/or codes of practice issued by the Information Commissioner or any relevant Central Government Body in relation to such Act;
"**Force Majeure Event**"	means any event outside the reasonable control of either Party affecting its performance of its obligations under this Agreement arising from acts, events, omissions, happenings or non-happenings beyond its reasonable control and which are not attributable to any wilful act, neglect or failure to take reasonable preventative action by that Party, including acts of God, riots, war or armed conflict, acts of terrorism, acts of government, local government or regulatory bodies, fire, flood, storm or earthquake, or disaster but excluding any industrial dispute relating to the Supplier or the Supplier Personnel or any other failure in the Supplier's or a Subcontractor's supply chain;
"**Force Majeure Notice**"	means a written notice served by the Affected Party on the other Party stating that the Affected Party believes that there is a Force Majeure Event;
"**Former Supplier**"	means a supplier supplying services to the Authority before the Relevant Transfer Date that are the same as or substantially similar to the Services (or any part of the Services) and shall include any subcontractor of such supplier (or any Sub-contractor of any such Sub-contractor)
"**GDPR**"	means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of Personal Data and repealing Directive 95/46/EC (General Data Protection Regulation) OJ L 119/1, 4.5.2016;
General AntiAbuse Rule"	means:- (a) the legislation in Part 5 of the Finance Act 2013; and (b) any future legislation introduced into parliament to counteract tax advantages arising from abusive arrangements to avoid national insurance contributions;
"**General Change in Law**"	means a Change in Law where the change is of a general legislative nature (including taxation or duties of any sort affecting the Supplier) or which affects or relates to a Comparable Supply;
"**Good Industry Practice**"	means at any time the exercise of that degree of care, skill, diligence, prudence, efficiency, foresight and timeliness which would be reasonably expected at such time from a leading and expert supplier of services similar to the Services to a customer like the Authority, such supplier seeking to comply with its contractual obligations in full and complying with applicable Laws;
"**Government Commercial Operating Standards" ("GCOS")**	means the Government Functional Standard - GovS 008: Commercial, as may be amended from time to time. The purpose of these standards is to set expectations and drive consistency in the planning, management and execution of commercial activities, ensuring contracts and relationships with suppliers realise value for money and result in delivery of high-quality public services. Further information is available at: https://www.gov.uk/government/publications/commercial-operating-standards-for-government.

"**Group Structure Information and Resolution Commentary**"	means the information relating to the Supplier Group to be provided by the Supplier in accordance with paragraphs 11 to 13 and Appendix 1 of Part 2 of Schedule 8.6 (*Service Continuity Plan*);
"**Halifax Abuse Principle**"	means the principle explained in the CJEU Case C-255/02 Halifax and others;
"**Health and Safety Policy**"	means the health and safety policy of the Authority, Service Recipients and/or other relevant Central Government Body as provided to the Supplier on or before the Effective Date and as subsequently provided to the Supplier from time to time except any provision of any such subsequently provided policy that cannot be reasonably reconciled to ensuring compliance with applicable Law regarding health and safety;
"**Help Desk**"	means the single point of contact help desk set up and operated by the Supplier for the purposes of this Agreement;
"**HMRC**"	means HM Revenue & Customs;
"**Impact Assessment**"	means an assessment of a Change Request in accordance with paragraph 4 of Schedule 8.2 (*Change Control Procedure*);
"**Impact Assessment Estimate**"	has the meaning given in paragraph 3.3 of Schedule 8.2 (*Change Control Procedure*);
"**Implementation Plan**"	means the Outline Implementation Plan or (if and when approved by the Authority pursuant to paragraph 3 of Schedule 6.1 (*Implementation Plan*)) the Detailed Implementation Plan as updated in accordance with paragraph 4 of Schedule 6.1 (*Implementation Plan*) from time to time;
"**Implementation Services**"	means the implementation services specified in the Services Description to ensure the Operational Services are ready to be provided with effect from the Operational Service Commencement Date;
"**Implementation Services Commencement Date**"	means the date on which the Supplier is to commence provision of the Implementation Services, being the date specified in the Implementation Plan;
"**Indemnified Person**"	means the Authority, each Service Recipient and each and every person to whom the Authority (or any direct or indirect sub-licensee of the Authority) sub-licenses, assigns or novates any Relevant IPRs or rights in Relevant IPRs where permitted to do so in accordance with this Agreement;
"**Indemnifier**"	has the meaning given in paragraph 1.1 of Schedule 8.7 (*Conduct of Claim*)
"**Indexation**" and "**Index**"	means the adjustment of an amount or sum in accordance with paragraph 10 of Part C of Schedule 7.1 (*Charges and Invoicing*);
"**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 CDROM, magnetic and digital form);
"**Information Commissioner**"	means the UK Information Commissioner (including any successor or replacement);
"**Information Management System**"	means the Core Information Management System and the Wider Information Management System;

"**Initial Term**" means the period of forty eight (48) months from and including the Implementation Services Commencement Date;

"**Insolvency Continuity Plan**" as the meaning given in paragraph 1.2.1(d) of Schedule 8.6 (*Service Continuity Plan*)

"**Insolvency Event**" means with respect to any person, means:-

(a) that person suspends, or threatens to suspend, payment of its debts, or is unable to pay its debts as they fall due or admits inability to pay its debts, or:-

(i) (being a company or a LLP) is deemed unable to pay its debts within the meaning of section 123 of the Insolvency Act 1986; or

(ii) (being a partnership) is deemed unable to pay its debts within the meaning of section 222 of the Insolvency Act 1986;

(b) that person commences negotiations with one or more of its creditors (using a voluntary arrangement, scheme of arrangement or otherwise) with a view to rescheduling any of its debts, or makes a proposal for or enters into any compromise or arrangement with one or more of its creditors or takes any step to obtain a moratorium pursuant to section 1A and Schedule A1 of the Insolvency Act 1986 other than (in the case of a company, a LLP or a partnership) for the sole purpose of a scheme for a solvent amalgamation of that that person with one or more other companies or the solvent reconstruction of that person;

(c) another person becomes entitled to appoint a receiver over the assets of that person or a receiver is appointed over the assets of that person;

(d) a creditor or encumbrancer of that person attaches or takes possession of, or a distress, execution or other such process is levied or enforced on or sued against, the whole or any part of that person's assets and such attachment or process is not discharged within fourteen (14) days;

(e) that person suspends or ceases, or threatens to suspend or cease, carrying on all or a substantial part of its business;

(f) where that person is a company, a LLP or a partnership:-

(i) a petition is presented (which is not dismissed within fourteen (14) days of its service), a notice is given, a resolution is passed, or an order is made, for or in connection with the winding up of that person other than for the sole purpose of a scheme for a solvent amalgamation of that person with one or more other companies or the solvent reconstruction of that person;

(ii) an application is made to court, or an order is made, for the appointment of an administrator, or if a notice of intention to appoint an administrator is filed at Court or given or if an administrator is appointed, over that person;

(iii) (being a company or a LLP) the holder of a qualifying floating charge over the assets of that person has become entitled to appoint or has appointed an administrative receiver; or

(iv) (being a partnership) the holder of an agricultural floating charge over the assets of that person has become entitled to appoint or has appointed an agricultural receiver; or

(g) any event occurs, or proceeding is taken, with respect to that person in any jurisdiction to which it is subject that has an effect equivalent or similar to any of the events mentioned above;

"**Intellectual Property Rights**" **or** "**IPRs**" means:-

(a) copyright, rights related to or affording protection similar to copyright, rights in databases, patents and rights in inventions, semiconductor topography rights, trade marks, rights in Internet domain names and website addresses and other rights in trade names, designs, knowhow, trade secrets and other rights in Confidential Information;

(b) applications for registration, and the right to apply for registration, for any of the rights listed at (a) that are capable of being registered in any country or jurisdiction; and

(c) all other rights having equivalent or similar effect in any country or jurisdiction;

"**IPRs Claim**" means any claim against any Indemnified Person of infringement or alleged infringement (including the defence of such infringement or alleged infringement) of any Relevant IPRs in respect of:

(a) rights granted to the Indemnified Persons under this Agreement;

(b) the Supplier's performance of the Services; and/or

(c) the use by the Authority and Service Recipients of the Services;

"**IT**" means information and communications technology;

"**IT Environment**" means the Authority System and the Supplier System;

"JCT contracts" means the range of building contracts to suit all projects and procurement options produced by The Joint Contracts Tribunal Limited;

"**Joint Implementation Board**" means the body described in paragraph 3 of Schedule 8.1 (*Governance*);

"**IT Health Check**" has the meaning given paragraph 14.1.1 of Schedule 2.4 (*Security Management*);

"**Key Performance Indicator**" means the key performance indicators set out in Table 1 of Part 1 of Appendix 1 of Schedule 2.2 (*Performance Levels*);

"**KPI Failure**" means a failure to meet the Target Performance Level in respect of a Key Performance Indicator;

"**KPI Service Threshold**"	has the meaning set out against the relevant Key Performance Indicator in Table 1 of Part 1 of Appendix 1 of Schedule 2.2 (*Performance Levels*);
"**Law**"	means any law, statute, subordinate legislation within the meaning of section 21(1) of the Interpretation Act 1978, bye-law, enforceable right within the meaning of section 2 of the European Communities Act 1972, regulation, order, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements of any regulatory body with which the Supplier is bound to comply;
"Licensed Data"	means any data that is not Authority Data, and includes, but is not limited to, publicly available data that is mined and compiled by Supplier, data shared by third parties for use by Supplier customers on the Supplier Solution, data acquired by Supplier from free or paid sources, event monitoring data, event history data, supplier information data, as well as content generated by Supplier such as performance and usage metrics, benchmarking, maturity models, best practices guides, Resilinc R Score and other derivative products. For avoidance of all doubt, all publicly available data that is consolidated by Supplier using Supplier resources is included in Licensed Data and is subject to restrictions on use as defined below. Company's use of Licensed Data is subject to terms and restrictions set forth in this Agreement.
"**Licensed Software**"	means all and any Software licensed by or through the Supplier, its Sub-contractors or any third party to the Authority for the purposes of or pursuant to this Agreement, including any Supplier Software and Third Party Software;
"List of Controlled Documents"	means the list at Appendix 3 (Initial List of Controlled Documents) of Schedule 8.2 (*Change Control Procedure*) as amended from time to time in accordance with paragraph 9 of that Schedule;
"Logged Issue"	means a problem or requirement notified to the Help Desk and logged on the Help Desk system with a reference number
"**Losses**" **or "Loss"**	means losses, liabilities, damages, costs and expenses (including legal fees on a solicitor/client basis) and disbursements and costs of investigation, litigation, settlement, judgment interest and penalties whether arising in contract, tort (including negligence), breach of statutory duty or otherwise;
"**Malicious Software**"	means any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on program files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed, and whether the malicious software is introduced wilfully, negligently or without knowledge of its existence;
"**Man Day**"	means 7.5 Man Hours, whether or not such hours are worked consecutively and whether or not they are worked on the same day
"**Man 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 or relevant Sub-contractor's offices, or to and from the Sites) but excluding lunch breaks.
"**Management Information**"	means the management information specified in Schedule 2.2 (*Performance Levels*) Schedule 7.1 (*Charges and Invoicing*) and Schedule 8.1 (*Governance*) to be provided by the Supplier to the Authority;
"**Material KPI Failure**"	means:-

(a) a Serious KPI Failure;

(b) a failure by the Supplier to meet a KPI Service Threshold;

"**Measurement Period**"	means in relation to a Key Performance Indicator, the period over which the Supplier's performance is measured (for example, a Service Period if measured monthly or a twelve (12) month period if measured annually);
"**Milestone**"	means an event or task described in the Implementation Plan or, with respect to an Additional Milestone, as agreed between the Parties through the Change Control Procedure which, if applicable, shall be completed by the relevant Milestone Date;
"**Mediation Notice**"	has the meaning given in paragraph 4.2 of Schedule 8.3 (*Dispute Resolution Procedure*);
"Mediator"	the independent third party appointed in accordance with paragraph 5.2 of Schedule 8.3 (*Dispute Resolution Procedure*) to mediate a Dispute.
"**Milestone Achievement Certificate**"	means the certificate to be granted by the Authority when the Supplier has Achieved a Milestone, which shall be in substantially the same form as that set out in Appendix 1 of Schedule 6.2 (*Milestone Achievement Procedure*);
"Milestone Achievement Procedure"	means the process for determining whether or a not a Milestone is Achieved as described in Schedule 6.2 (*Milestone Achievement Procedure*);
"**Milestone Date**"	means the target date set out against the relevant Milestone in the Implementation Plan or (with respect to an Additional Milestone) as agreed between the Parties under the Change Control Procedure by which the Milestone must be Achieved;
"**Milestone Payment**"	means a payment identified in Schedule 7.1 (*Charges and Invoicing*) (or, with respect to an Additional Milestone, as agreed between the Parties under the Change Control Procedure) to be made following the issue of a Milestone Achievement Certificate;
"**Minor KPI Failure**"	means shall be as set out against the relevant Key Performance Indicator in Table 1 of Part 1 of Appendix 1 of Schedule 2.2 (*Performance Levels*);
"Mitigated"	Means a vulnerability has been either removed or put in such a state as to not be relevant;
"**month**"	means a calendar month and "**monthly**" shall be interpreted accordingly;
"**Multi-Party Dispute**"	a Dispute which involves the Parties and one or more Related Third Parties.
"**Multi-Party Dispute Resolution Procedure**"	has the meaning given in paragraph 9.1 of Schedule 8.3 (*Dispute Resolution Procedure*);
"**Multi-Party Dispute Representatives**"	has the meaning given in paragraph 9.6 of Schedule 8.3 (*Dispute Resolution Procedure*);
"**Multi-Party Dispute Resolution Board**"	has the meaning given in paragraph 9.6 of Schedule 8.3 (*Dispute Resolution Procedure*);
"**Multi-Party Procedure Initiation Notice**"	has the meaning given in paragraph 9.2 of Schedule 8.3 (*Dispute Resolution Procedure*);

"NEC"	means the range of contracts designed to manage projects from start to finish produced by the Institute of Civil Engineers;
"**Net Book Value**"	the net book value of the relevant Asset(s) calculated in accordance with the depreciation policy of the Supplier set out in the letter in the agreed form from the Supplier to the Authority of the same date as this Agreement;
"**New Releases**"	means an item produced primarily to extend, alter or improve the Software and/or any Deliverable by providing additional functionality or performance enhancement (whether or not defects in the Software and/or Deliverable are also corrected) while still retaining the original designated purpose of that item;
"**Non-Available**"	means in relation to the IT Environment or the Services, that the IT Environment or the Services are not Available
"Non-Chargeable Change"	has the meaning given to it in paragraph 2.3.2 of Schedule 8.2 (*Change Control Procedure*);
"**Non-Exclusive Assets**"	those Assets (if any) which are used by the Supplier or a subcontractor in connection with the provision of the Services but which are also used by the Supplier or subcontractor for other purposes of material value;
"**Non-trivial Customer Base**"	means a significant customer base with respect to the date of first release and the relevant market but excluding Affiliates and other entities related to the licensor;
"**Notifiable Default**"	shall have the meaning given in Clause 26.1 (*Rectification Plan Process*);
"**Occasion of Tax Non-Compliance**"	means:- (a) any tax return of the Supplier submitted to a Relevant Tax Authority on or after 1 October 2012 is found on or after 1 April 2013 to be incorrect as a result of:- (i) a Relevant Tax Authority successfully challenging the Supplier under the General Anti-Abuse Rule or the Halifax Abuse Principle or under any tax rules or legislation that have an effect equivalent or similar to the General Anti-Abuse Rule or the Halifax Abuse Principle; (ii) the failure of an avoidance scheme which the Supplier was involved in, and which was, or should have been, notified to a Relevant Tax Authority under the DOTAS or any equivalent or similar regime; and/or (b) any tax return of the Supplier submitted to a Relevant Tax Authority on or after 1 October 2012 gives rise on or after 1 April 2013 to a criminal conviction in any jurisdiction for tax related offences which is not spent at the Effective Date or to a civil penalty for fraud or evasion;
"**Open Source**"	means computer Software that is released on the internet for use by any person, such release usually being made under a recognised open source licence and stating that it is released as open source;
"**Operating Environment**"	means the environment in which the Services will be used by the Authority and the Service Recipients including the Authority System and the Sites;

"**Operational Change**"	means any change in the Supplier's operational procedures which in all respects, when implemented:- (a) will not affect the Charges and will not result in any other costs to the Authority; (b) will not require a change to this Agreement; (c) may change the way in which the Services are delivered but will not adversely affect the output of the Services or increase the risks in performing or receiving the Services; and (d) will not adversely affect the interfaces or interoperability of the Services with any of the Authority's IT infrastructure or the services or infrastructure provided by an Other Supplier;
"**Operational Service Commencement Date**"	means in relation to an Operational Service the date identified in the Implementation Plan upon which the Operational Services are to commence;
"**Operational Services**"	means the operational services described as such in the Services Description;
"Optional Services"	means the provision of the Optional Services listed in Appendix 2 of Schedule 7.1 (*Charges and Invoicing*).
"**Ordinary Exit**"	Means any termination of the whole or part of this Agreement which occurs pursuant to Clause 33 (*Termination Rights)* where the period of notice given by the Party serving notice to terminate pursuant to such Clause is greater than or equal to six (6) months; or as a result of the expiry of the Initial Term or any Extension Period;
"**Other Supplier**"	means any supplier to the Authority, the Service Recipients and/or the Department of Business, Energy and Industrial Strategy or its successor body (other than the Supplier), including any supplier relevant to the delivery of Project Victory, which is notified to the Supplier by the Authority from time to time;
"**Outline Implementation Plan**"	means the outline plan set out at Appendix 1 of Schedule 6.1 (*Implementation Plan*);
"**Overhead**"	means those amounts which are intended to recover a proportion of the Supplier's or the subcontractor'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 paragraph (a) of the definition of "**Costs**" or the day cost set out in Table 11 of Appendix 3 of Schedule 7.1 (*Charges and Invoicing*);
"**Parent Undertaking**"	has the meaning set out in section 1162 of the Companies Act 2006;
"**Partial Termination**"	means the partial termination of this Agreement to the extent that it relates to the provision of any part of the Services as further provided for in Clause 29.2.3 (*Termination by the Authority*) or otherwise by mutual agreement by the Parties.
"**Parties**" and "**Party**"	have the meanings respectively given on page 1 of this Agreement

"**Performance Monitoring Report**"	has the meaning given in paragraph 1.1.1 of Part 2 of Schedule 2.2 *(Performance Levels);*
"**Performance Review Meeting**"	means the regular meetings between the Supplier and the Authority to manage and review the Supplier's performance under this Agreement, as further described in paragraph 1.3 of Part 2 of Schedule 2.2 *(Performance Levels)*;
"Permitted Maintenance"	shall have the meaning in paragraph 4 of part 1 of Schedule 2.2 *(Performance Levels)*.
"**Personal Data**"	has the meaning given in the Data Protection Legislation and for the purposes of this Agreement includes special categories of Personal Data as set out in Article 9 of the GDPR and personal data relating to criminal convictions and offences as described in Article 10 of the GDPR;
"**Personal Data Breach**"	has the meaning given in the Data Protection Legislation;
"**Personal Data Processing Statement**"	sets out: (i) the types of Personal Data which the Supplier and/or its Subcontractors are Processing on behalf of the Authority; (ii) the categories of Data Subjects whose Personal Data the Supplier and/or its Subcontractors are Processing on behalf of the Authority; the nature and purpose of such Processing; (iii) the locations at which the Supplier and/or its Sub-contractors Process Authority Data; and, (iv) the Protective Measures that the Supplier and, where applicable, its Sub-contractors have implemented to protect the Authority Data against a Security Breach including a Personal Data Breach, which shall be prepared by the Supplier in accordance with paragraph 5.4 of Schedule 2.4 *(Security Management*) and included in the Risk Management Documentation;
"**Process**", "**Processed**" or "**Processing**"	have the meaning given in the Data Protection Legislation;
"**Process Authority Data**"	means any operation which is performed on Authority Data, whether or not by automated means, including adapting, altering, collecting, combining, copying, destroying, erasing, handling, organising, publishing retrieving, storing, structuring, transmitting or otherwise using Authority Data;
"**Processor**"	has the meaning given in the Data Protection Legislation;
"**Product Roadmap**"	means the roadmap for the Licensed Software that the Supplier (or its licensors) maintains from time to time that shall include:- (a) details of the new or revised functionality of the Licensed Software taking into account the version of the Licensed Software that is available in the market from time to time; (b) mapping against relevant industry standards; (c) the key characteristics and benefits of the Licensed Software;

(d) the Licensed Software's ability to interoperate with the Authority's interfacing systems including the software of the Other Suppliers; and

(e) any modifications that might be required to existing Vehicle design and installations;

"**Prohibited Act**" means:-

(a) to directly or indirectly offer, promise or give any person working for or engaged by the Authority or a Service Recipient a financial or other advantage to:-

(i) induce that person to perform improperly a relevant function or activity; or

(ii) reward that person for improper performance of a relevant function or activity;

(b) to directly or indirectly request, agree to receive or accept any financial or other advantage as an inducement or a reward for improper performance of a relevant function or activity in connection with this Agreement;

(c) an offence:-

(i) under the Bribery Act 2010 (or any legislation repealed or revoked by such Act);

(ii) under legislation or common law concerning fraudulent acts (including offences by the Supplier under Part 3 of the Criminal Finances Act 2017); or

(iii) defrauding, attempting to defraud or conspiring to defraud the Authority or a Service Recipient; or

(d) any activity, practice or conduct which would constitute one of the offences listed under (c) above if such activity, practice or conduct had been carried out in the UK;

"**Project**" means a one-time activity to be supplied by the Supplier that has been commissioned under the Change Control Procedure;

"**Project Charges**" means the Charges for delivery of a Project as set out in the relevant Change Authorisation Notice based on the charging principles for Projects set out in Schedule 7.1 (*Charges and Invoicing*);

"**Project Managers**" means the individuals appointed as such by the Authority and the Supplier in accordance with paragraph 1 of Schedule 8.1 (*Governance*);

"**Project Victory**" means the programme of procurements that the Authority initiated pursuant to the FTS notice referred to in Recital (B);

"**Public Sector Dependent Supplier**" means a supplier where that Supplier, or that Supplier's Group has Annual Revenue of £50 million or more of which over 50% is generated from UK Public Sector Business;

"**Public Sector and CNI Contract Information**" means the information requirements set out in accordance with Appendix 2 of Part 2 of Schedule 8.6 (*Service Continuity Plan*);

"**Quarter**"	means the first three Service Periods and each subsequent three Service Periods (save that the final Quarter shall end on the date of termination or expiry of this Agreement);
"**Receiving Party**"	means the Party which receives a proposed Contract Change;
"**Recipient**"	has the meaning given in Clause 20.1 (*Confidentiality*);
"**Records**"	has the meaning given in Schedule 8.4 (*Reports and Records Provisions*);
"**Rectification Plan**"	means a plan to address the impact of, and prevent the reoccurrence of, a Notifiable Default;
"**Rectification Plan Failure**"	(a) the Supplier failing to submit or resubmit a draft Rectification Plan to the Authority within the timescales specified in Clauses 26.4 (*Submission of the draft Rectification Plan*) or 26.8 (A*greement of the Rectification Plan*); (b) the Authority, acting reasonably, rejecting a revised draft of the Rectification Plan submitted by the Supplier pursuant to Clause 26.7 (*Agreement of the Rectification Plan*); (c) the Supplier failing to rectify a material Default within the later of:- (i) thirty (30) Working Days of a notification made pursuant to Clause 26.2 (*Notification*); and (ii) where the Parties have agreed a Rectification Plan in respect of that material Default and the Supplier can demonstrate that it is implementing the Rectification Plan in good faith, the date specified in the Rectification Plan by which the Supplier must rectify the material Default; (d) a Material KPI Failure reoccurring in respect of the same Key Performance Indicator for the same (or substantially the same) root cause in any of the three (3) Measurement Periods subsequent to the Measurement Period in which the initial Material KPI Failure occurred; (e) the Supplier not Achieving the Milestone for Operational Services Commencement Date within thirty (30) days of the date on which it is planned to be Achieved (as specified in the Implementation Plan); and/or (f) following the successful implementation of a Rectification Plan, the same Notifiable Default recurring within a period of six (6) months for the same (or substantially the same) root cause as that of the original Notifiable Default;
"**Rectification Plan Process**"	means the process set out in Clauses 26.4 (*Submission of the draft Rectification Plan*) to 26.9 (*Agreement of the Rectification Plan*);
"**Register**"	Means the register and configuration database referred to in paragraphs 2.1.1 and 2.1.2 of Schedule 8.5 (*Exit Management);*
"**Regulator Correspondence**"	means any correspondence from the Information Commissioner or other applicable regulator in relation to the Processing of Personal Data;
"**Reimbursable Expenses**"	means reasonable out of pocket travel and subsistence (for example, hotel and food) expenses, properly and necessarily incurred in the provision of the

Services, calculated at the rates and in accordance with the Authority'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 Authority otherwise agrees in advance in writing and
b. subsistence expenses incurred by Supplier Personnel whilst providing the Services at their usual place of work, or to and from the premises at which the Services are principally to be performed.

"**Related Third Party**"	means a party to:- a. another contract with the Authority or the Supplier which is relevant to this Agreement or b. a Subcontract.
"**Related Service Provider**"	means any person who provides services to the Authority or any Service Recipient in relation to this Agreement from time to time;
"**Relevant Authority**"	means the Authority or, where the Supplier is a Strategic Supplier, the Cabinet Office Markets and Suppliers Team;
"**Relevant IPRs**"	means IPRs used to provide the Services or as otherwise provided and/or licensed by the Supplier (or to which the Supplier has provided access) to the Authority or a third party in the fulfilment of the Supplier's obligations under this Agreement including IPRs in the Licensed Software;
"**Relevant Requirements**"	means all applicable Law relating to bribery, corruption and fraud, including the Bribery Act 2010 and any guidance issued by the Secretary of State for Justice pursuant to section 9 of the Bribery Act 2010;
"**Relevant Tax Authority**"	means HMRC, or, if applicable, a tax authority in the jurisdiction in which the Supplier is established;
"**Relevant Transfer**"	means a transfer of employment to which the Employment Regulations applies;
"**Relevant Transfer Date**"	means in relation to a Relevant Transfer, the date upon which the Relevant Transfer takes place
"**Relief Notice**"	has the meaning given in Clause 27.2 (*Authority Cause*);
"**Repeat KPI Failure**"	has the meaning given in paragraph 3.1 of Part 1 of Schedule 2 (*Performance Levels);*
"**Replacement Services**"	means any services which are the same as or substantially similar to any of the Services and which the Authority or a Service Recipient receives in substitution for any of the Services following the expiry or termination or Partial Termination of this Agreement, whether those services are provided by the Authority or a Service Recipient internally and/or by any third party;
"**Replacement Supplier**"	means any third party service provider of Replacement Services appointed by the Authority or a Service Recipient from time to time (or where the Authority or Service Recipient is providing replacement Services for its own account, the Authority or Service Recipient);

"**Replacement sub-contractor"**	means a Sub-contractor of the Replacement Supplier to whom Transferring Supplier Employees will transfer on a Service Transfer Date (or any Sub-contractor of any such Sub-contractor)
"**Request for Estimate**"	a written request sent by the Authority to the Supplier, requiring that the Supplier provide it with an accurate estimate of the Termination Payment that would be payable if the Authority exercised its right under Clause 31.1.1 (*Termination by the Authority*) to terminate this Agreement for convenience on a specified Termination Date;
"**Request For Information**"	means a Request for Information under the FOIA or the EIRs;
"**Required Changes Register**"	is a register which forms part of the Risk Management Documentation which records each of the changes that the Supplier has agreed with the Authority shall be made to the Core Information System and/or the Risk Management Documentation as a consequence of the occurrence of any of the events set out in paragraph 5.13.1 to 5.13.8 of Schedule 2.4 (*Security Management*) together with the date on which each such change shall be implemented and the date on which each such change was implemented;
"**Review Report**"	has the meaning given in paragraphs 6.2.1 to 6.2.3 of Schedule 8.6 (*Service Continuity Plan*);
"**Risk Management Approval Statement**"	is a notice issued by the Authority which sets out the information risks associated with using the Core Information Management System and confirms that the Authority is satisfied that the identified risks have been adequately and appropriately addressed and that the residual risks are understood and accepted by the Authority;
"**Risk Management Documentation**"	has the meaning given in paragraph 5.3 of Schedule 2.4 (*Security Management*);
"**Risk Management Reject Notice**"	as the meaning given in paragraph 5.7.2 of Schedule 2.4 (*Security Management*);
	[Redacted for Publication]
"**Satisfaction Survey**"	has the meaning given in paragraph 7.1 of Part 2 of Appendix 1 of Schedule 2.2. (*Performance Levels*);
"**Second Extension Period**"	means a period of twenty-four (24) months from the end of the First Extension Period;
"**Security Test**"	has the meaning given in paragraph 7.1 of Schedule 2.4 (*Security Management*);
"**Sensitive Claim**"	has the meaning given in paragraph 2.1 of Schedule 8.7 (*Conduct of Claim);*
"**Serious KPI Failure**"	shall be as set out against the relevant Key Performance Indicator in Table 1 of Part 1 of Appendix 1 of Schedule 2.2 (*Performance Levels*);
"**Service Availability**"	has the meaning given in paragraph 2 of Part 2 of Appendix 1 of Schedule 2.2 (*Performance Levels*);
"**Service Charges**"	means the periodic payments made in accordance with Schedule 7.1 (*Charges and Invoicing*) in respect of the supply of the Operational Services;

"**Service Continuity Plan**"	means, as at the Effective Date, the plan attached at Appendix 1 of Schedule 8.6 (*Service Continuity Plan*) and as updated pursuant to paragraph 6 of that Schedule which incorporates the Business Continuity Plan, Disaster Recovery Plan and the Insolvency Continuity Plan;
"**Service Continuity Services**"	means the business continuity, disaster recovery and insolvency continuity services set out in Schedule 8.6 (*Service Continuity Plan*);
"**Service Credits**"	means credits payable by the Supplier due to the occurrence of 1 or more KPI Failures, calculated in accordance with paragraph 8 of Part C of Schedule 7.1 (*Charges and Invoicing*);
"**Service Downtime**"	means any period of time during which any of the Services are not Available
"**Service Incident**"	means a reported occurrence of a failure to deliver any part of the Services in accordance with the Authority Requirements or the Key Performance Indicators
"**Service Period**"	means a calendar month, save that:- (a) the first service period shall begin on the first Operational Service Commencement Date and shall expire at the end of the calendar month in which the first Operational Service Commencement Date falls; and (b) the final service period shall commence on the first day of the calendar month in which the Term expires or terminates and shall end on the expiry or termination of the Term
"**Service Points**"	means in relation to a KPI Failure, the points that are set out against the relevant Key Performance Indicator in the Service Points column of Table in Appendix 1 of Schedule 2.2 (*Performance Levels*);
"**Service Recipient**"	means each of: (a) Sellafield Limited a company registered in England and Wales (company number 01002607) with its registered office at Hinton House Birchwood Park Avenue, Risley, Warrington, Cheshire, United Kingdom, WA3 6GR; (b) Low Level Waste Repository Ltd a company registered in England and Wales (company number 05608448) with its registered office at Old Shore Road, Drigg, Holmrook, Cumbria, CA19 1XH; (c) Magnox Limited a company registered in England and Wales (company number 02264251) with its registered office at Oldbury Technical Centre, Oldbury Naite, Thornbury, South Gloucestershire, England, BS35 1RQ; (d) Dounreay Site Restoration Limited a company registered in Scotland (company number SC307493) with its registered office at Building D2003, Dounreay, Thurso, Caithness, KW14 7TZ; (e) International Nuclear Services Limited a company registered in England and Wales (company number 01144352) with its registered office at Herdus House Ingwell Drive, Westlakes Science & Technology Park, Moor Row, Cumbria, CA24 3HU; (f) Direct Rail Services Limited a company registered in England and Wales (company number 03020822) with its registered office at Herdus House Ingwell Drive, Westlakes Science & Technology Park, Moor Row, Cumbria, CA24 3HU;

(g) Radioactive Waste Management Limited a company registered in England and Wales (company number 08920190) with its registered office at Building 329 West Thomson Avenue, Harwell Oxford, Didcot, England, OX11 0GD;

(h) Rutherford Indemnity Limited a company registered in Guernsey and regulated by the Guernsey Financial Services Commission;

(i) Nuclear Decommissioning Authority with its office at Herdus House Ingwell Drive, Westlakes Science & Technology Park, Moor Row, Cumbria, CA24 3HU;

(j) National Nuclear Laboratory Limited a company registered in England and Wales (company number 03857752) with its registered office at Chadwick House Warrington Road, Birchwood Park, Warrington, WA3 6AE;

(k) the Office of the Nuclear Regulator;

(l) any other UK public sector contracting authority that delivers services to the UK in respect of the nuclear decommissioning programme; and

(m) any person that is owned or controlled by the Department for Business, Energy and Industrial Strategy, the Authority or any of the entities listed at paragraphs (a) to (l) above,

and any successor bodies thereto that perform any of the functions previously performed by any of the foregoing bodies;

"**Service Transfer**" means any transfer of the Services (or any part of the Services), for whatever reason, from the Supplier or any Sub-contractor to a Replacement Supplier or a Replacement Sub-contractor;

"**Service Transfer Date**" means the date of a Service Transfer or, if more than one, the date of the relevant Service Transfer as the context requires;

"**Services**" means any and all of the services to be provided by the Supplier under this Agreement, including those set out in Schedule 2.1 (*Services Description*);

"**Services Description**" means the services description set out in Schedule 2.1 (*Services Description*);

"Severity Level 1" Production application down or major malfunction resulting in a product inoperative condition. Users unable to reasonably perform their normal functions.

"**Sites**" means any premises (including the Authority Premises, the Supplier's premises or third party premises"):-

(a) from, to or at which:-

(i) the Services are (or are to be) provided; or

(ii) the Supplier manages, organises or otherwise directs the provision or the use of the Services; or

(b) where:-

(i) any part of the Supplier System is situated; or

(ii) any physical interface with the Authority System takes place;

"**SME**" **or "Small and Medium-sized Enterprises"**	means an enterprise falling within the category of micro, small and medium-sized enterprises defined by the Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises;
"**Software**"	means Supplier Software and Third Party Software;
"**Specific Change in Law**"	means a Change in Law that relates specifically to the business of the Authority and which would not affect a Comparable Supply;
"**Staffing Information**"	means in relation to all persons identified on the Supplier's Provisional Supplier Personnel List or Supplier's Final Supplier Personnel List, as the case may be, such information as the Authority may reasonably request (subject to all applicable provisions of the DPA), but including in an anonymised format: a. their ages, dates of commencement of employment or engagement, gender and place of work b. details of whether they are employed, self employed contractors or consultants, agency workers or otherwise c. the identity of the employer or relevant contracting Party d. their relevant contractual notice periods and any other terms relating to termination of employment, including redundancy procedures, and redundancy payments e. their wages, salaries, bonuses and profit sharing arrangements as applicable f. details of other employment-related benefits, including (without limitation) medical insurance, life assurance, pension or other retirement benefit schemes, share option schemes and company car schedules applicable to them g. any outstanding or potential contractual, statutory or other liabilities in respect of such individuals (including in respect of personal injury claims) h. details of any such individuals on long term sickness absence, parental leave, maternity leave or other authorised long-term absence i. copies of all relevant documents and materials relating to such information, including copies of relevant contracts of employment (or relevant standard contracts if applied generally in respect of such employees) and j. any other "employee liability information" as such term is defined in regulation 11 of the Employment Regulations;
"**Standard Contractual Clauses**"	means any valid standard data protection clauses appropriate to the applicable Data Subjects involved that may be adopted and approved by the European Commission or the UK Government including the EU Standard Contractual Clauses adopted by Implementing Decision (EU) 2021/914 of 04 June 2021 or any additional replacement clauses approved by the European Commission from time to time and the International Data Transfer

	Agreement adopted by UK Parliament on 21 March 2022 or any additional replacement clauses approved by the UK Government from time to time
"**Standards**"	the standards, polices and/or procedures identified in Schedule 2.3 (*Standards*);
"**Standards Hub**"	means the Government's open and transparent standards adoption process as documented at http://standards.data.gov.uk/
"**Statement of Information Risk Appetite**"	has the meaning given paragraph 4.1 of Schedule 2.4 *(Security Management)*;
"**Strategic Supplier**"	means those suppliers to government listed at https:-//www.gov.uk/government/publications/strategic-suppliers;
"**Subcontract**"	means any contract or agreement (or proposed contract or agreement) between the Supplier (or a Sub-contractor) and any third party whereby that third party agrees to provide to the Supplier (or the Sub-contractor) all or any part of the Services or facilities or services which are material for the provision of the Services or any part thereof or necessary for the management, direction or control of the Services or any part thereof;
"**Subcontractor**"	means any third party (including a sub-processor of Authority Personal Data) with whom:- (a) the Supplier enters into a Subcontract; or (b) a third party under (a) above enters into a Sub-contract, or the servants or agents of that third party;
"**Subsidiary Undertaking**"	has the meaning set out in section 1162 of the Companies Act 2006;
"**Successor Body**"	has the meaning given in Clause 32.4 (*Assignment and Novation*);
"**Suggested Challenge**"	means a submission to suggest the adoption of new or emergent standards in the format specified on Standards Hub
"**Supplier Change Manager**"	means the person appointed to that position by the Supplier from time to time and notified in writing to the Authority or, if no person is notified, the Supplier Representative;
"**Supplier COTS IPRs**"	means any embodiments of Supplier IPRs that are COTS;
"**Supplier COTS Software**"	means Supplier Software (including open source software) that is COTS;
"Supplier Forum"	means the body described in paragraph 5 of Schedule 8.1 (*Governance*);
"**Supplier Group**"	means the Supplier, its Dependent Parent Undertakings and all Subsidiary Undertakings and Associates of such Dependent Parent Undertakings;
"**Supplier IPRs**"	means:- (a) Intellectual Property Rights owned by the Supplier (or an Affiliate of the Supplier) before or after the Effective Date, for example those subsisting in the Supplier's or Affiliate's standard development tools, program components or standard code used in computer programming or in physical or electronic media containing the

Supplier's or Affiliate's know-how or generic business methodologies; and/or

(b) Intellectual Property Rights created by the Supplier (or an Affiliate of the Supplier) independently of this Agreement,

which in each case is or will be used before or during the Term for designing, testing implementing or providing the Services but excluding Intellectual Property Rights owned by the Supplier (or Affiliate of the Supplier) subsisting in the Supplier Software;

"**Supplier NonCOTS IPRs**" means any embodiments of Supplier IPRs that have been delivered by the Supplier to the Authority and that are not Supplier COTS IPRs;

"**Supplier NonCOTS Software**" means Supplier Software that is not Supplier COTS Software;

"**Supplier NonPerformance**" has the meaning given in Clause 27.1 (*Authority Cause*);

"**Supplier Personnel**" means all directors, officers, employees, agents, consultants and contractors of the Supplier and/or of any Sub-contractor engaged in the performance of the Supplier's obligations under this Agreement;

"**Supplier Representative**" means the representative appointed by the Supplier pursuant to Clause 10.2 (*Representatives*), as notified to the Authority from time to time;

"**Supplier Request**" a notice served by the Supplier requesting that the Dispute be treated as a Multi-Party Dispute, setting out its grounds for that request and specifying each Related Third Party that it believes should be involved in the Multi-Dispute Resolution Procedure in respect of that Dispute.

"**Supplier Software**" means software which is proprietary to the Supplier (or an Affiliate of the Supplier) and which is or will be used by the Supplier for the purposes of providing the Services, including the software specified as such in Schedule 5 (*Software)*;

"**Supplier Solution**" means the Supplier's solution for the Services set out in Schedule 4.1 (*Supplier Solution*) including any Appendices of that Schedule;

"**Supplier System**" means the information and communications technology system used by the Supplier in implementing and performing the Services including the Software, the Supplier equipment, configuration and management utilities, calibration and testing tools and related cabling (but excluding the Authority System);

"**Supplier Termination Event**" means:-

(a) the Supplier's level of performance constituting a Critical Performance Failure;

(b) the Supplier committing a material Default which is irremediable;

(c) as a result of the Supplier's Default, the Authority incurring Losses in any Contract Year which exceed 80% of the value of any of the aggregate annual liability caps for that Contract Year as set out in Clause 24.3 (*Financial Limits*);

(d) a Rectification Plan Failure;

(e) where a right of termination is expressly reserved in this Agreement, including pursuant to:-

(i) Clause 18 (*IPRs Indemnity*);

(ii) Clause 35.6.2 (*Prevention of Fraud and Bribery*); and/or

(iii) Clause **Error! Reference source not found.** (*Financial Reporting and Assurance*);

(iv) paragraph 3 of Part 2 to Schedule 8.6 (*Service Continuity Plan*);

(f) the representation and warranty given by the Supplier pursuant to Clause 3.2.7 (*Warranties*) being materially untrue or misleading;

(g) the Supplier committing a material Default under Clause 9.10 (*Promoting Tax Compliance*) or failing to provide details of steps being taken and mitigating factors pursuant to Clause 9.10 (*Promoting Tax Compliance*) which in the reasonable opinion of the Authority are acceptable;

(h) the Supplier committing a material Default under any of the following Clauses:-

(i) Clause 20 (*Confidentiality*); and

(ii) Clause 21 (*Transparency and Freedom of Information*);

(iii) Clause 22 (*Protection of Personal Data*); and

(iv) Clause 31 (*Compliance*); and/or

in respect of any security requirements set out in Schedule 2.1 (*Services Description*), Schedule 2.4 (*Security Management*) or the Baseline Security Requirements; and/or

(i) an Insolvency Event occurring in respect of the Supplier;

(j) a change of Control of the Supplier unless:-

(i) the Authority has given its written consent to the particular Change of Control, which subsequently takes place as proposed; or

(ii) the Authority has not served its notice of objection within six (6) months of the later of the date on which the Change of Control took place or the date on which the Authority was given notice of the Change of Control;

(k) the Authority has become aware that the Supplier should have been excluded under Regulation 57(1) or (2) of the Public Contracts Regulations 2015 from the procurement procedure leading to the award of this Agreement;

(l) a failure by the Supplier to comply in the performance of the Services with legal obligations in the fields of environmental, social or labour law; or

"**Supplier's Final Supplier Personnel List**"	means a list provided by the Supplier of all Supplier Personnel who will transfer under the Employment Regulations on the Service Transfer Date
"**Supplier's Provisional Supplier Personnel List**"	means a list prepared and updated by the Supplier of all Supplier Personnel who are at the date of the list wholly or mainly engaged in or assigned to the provision of the Services or any relevant part of the Services which it is envisaged as at the date of such list will no longer be provided by the Supplier
"Supplier's Proposals"	has the meaning given to it in paragraph 6.2.3 of Schedule 8.6 (*Service Continuity Plan)*;
"**Supply Chain Transparency Report**"	means the report provided by the Supplier to the Authority in the form set out in Appendix 4 of Schedule 8.4 (*Reports and Records Provisions*);
"**Supporting Documentation**"	means sufficient information in writing to enable the Authority reasonably to assess whether the Charges, Reimbursable Expenses and other sums due from the Authority detailed in the information are properly payable, including copies of any applicable Milestone Achievement Certificates or receipts.
"**System Response Time**"	has the meaning given in paragraph 3.1 of Part 2 of Appendix of Schedule 2.2. (*Performance Levels*);
"**Target Performance Level**"	means the minimum level of performance for a Key Performance Indicator which is required by the Authority, as set out against the relevant Key Performance Indicator in the tables in Appendix 1 of Schedule 2.2 (*Performance Levels*);
"**Tender Documents**"	means the advertisement issued by the Authority seeking expressions of interest, the selection questionnaire, Invitation to Submit Initial Tender;
"**Term**"	means the period commencing on the Effective Date and ending on the expiry of the Initial Term or any Extension Period or on earlier termination of this Agreement;
"**Termination Assistance Notice**"	has the meaning given in paragraph 4.1 of Schedule 8.5 (*Exit Management)*;
"**Termination Assistance Period**"	means, in relation to a Termination Assistance Notice, the period specified in the Termination Assistance Notice for which the Supplier is required to provide the Termination Services as such period may be extended pursuant to paragraph 4.2 of Schedule 8.5 *(Exit Management*);
"**Termination Date**"	means the date set out in a Termination Notice on which this Agreement (or a part of it as the case may be) is to terminate;
"**Termination Estimate**"	has the meaning given in paragraph 10.2 of Schedule 7.2 (*Payments on Termination*);
"**Termination Notice**"	means a written notice of termination given by one Party to the other, notifying the Party receiving the notice of the intention of the Party giving the notice to terminate this Agreement (or any part thereof) on a specified date and setting out the grounds for termination;
"Termination Payment"	has the meaning given in paragraph 2 of Schedule 7.2 (P*ayments on Termination*);

"**Termination Services**"	means the services and activities to be performed by the Supplier pursuant to the Exit Plan, including those activities listed in Appendix 1 of Schedule 8.5 (*Exit Management*), and any other services required pursuant to the Termination Assistance Notice;
"**Tests**" and "**Testing**"	means any tests required to be carried out under this Agreement, as further described in the Implementation Plan or a Change Authorisation Note (as applicable); and "**Tested**" shall be construed accordingly;
"**Third Party Beneficiary**"	has the meaning given in Clause 39.1 (*Third Party Rights*);
"Third Party Contract"	means a contract with a third party entered into by the Supplier exclusively for the purpose of providing the Services, as listed in Schedule 4.2 (*Third Party Contracts*);
"**Third Party COTS IPRs**"	means Third Party IPRs that is COTS;
"**Third Party COTS Software**"	means Third Party Software (including open source software) that is COTS;
"**Third Party IPRs**"	means Intellectual Property Rights owned by a third party but excluding Intellectual Property Rights owned by the third party subsisting in any Third Party Software;
"**Third Party NonCOTS IPRs**"	means Third Party IPRs that are not Third Party COTS IPRs;
"**Third Party NonCOTS Software**"	means Third Party Software that is not Third Party COTS Software;
"**Third Party Provisions**"	has the meaning given in Clause 39.1 (*Third Party Rights*);
"**Third Party Software**"	means software which is proprietary to any third party (other than an Affiliate of the Supplier) or any Open Source Software which in any case is, will be or is proposed to be used by the Supplier for the purposes of providing the Services, including the software specified as such in Schedule 5 (*Software*);
"Time Service Charges"	means the charges relating to the Rate Card of Appendix 3 of Schedule 7.1 (*Charges and Invoicing*);
"**Transferable Assets**"	those of the Exclusive Assets which are capable of legal transfer to the Authority;
"**Transferable Contracts**"	means the Sub-contracts, licences for Supplier's Software, licences for Third Party Software or other agreements which are necessary to enable the Authority, any Service Recipient or any Replacement Supplier to provide the Services or the Replacement Services, including in relation to licences all relevant Documentation;
"**Transferring Assets**"	has the meaning given in paragraph 5.2,1 of Schedule 8.5 (*Exit Management*);
"**Transferring Contracts**"	has the meaning given in paragraph 5.2.1(c) of Schedule 8.5 (*Exit Management*)
"**Transferring Supplier Employees**"	means those employees of the Supplier and/or the Supplier's Sub-contractors to whom the Employment Regulations will apply on the Service Transfer Date;
"**UK**"	means the United Kingdom;

"**UK GDPR**"	means the EU GDPR as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 and as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 as amended or replaced from time to time;
"Unplanned System Downtime"	means any period of time during which any of the Services are not available, excluding Permitted Maintenance time;
"**Unrecovered Costs**"	means the Costs incurred by the Supplier in the performance of this Agreement (as summarised in the Financial Model) to the extent that the same remain at the Termination Date to be recovered through Charges that but for the termination of this Agreement would have been payable by the Authority after the Termination Date in accordance with Schedule 7.1 (*Charges and Invoicing*) as such Costs and Charges are forecast in the Financial Model;
"**Unrecovered Payment**"	means an amount equal to the lower of:- a. the sum of the Unrecovered Costs and b. the amount specified in paragraph 4.3 of Schedule 7.2 (*Payments on Termination*);
"**Updates**"	means in relation to any Software and/or any Deliverable means a version of such item which has been produced primarily to overcome Defects in, or to improve the operation of, that item;
"**Upgrades**"	means any patch, New Release or upgrade of Software and/or a Deliverable, including standard upgrades, product enhancements, and any modifications, but excluding any Update which the Supplier or a third party software supplier (or any Affiliate of the Supplier or any third party) releases during the Term;
"**VAT**"	means value added tax as provided for in the Value Added Tax Act 1994; and
"**Vulnerability Correction Plan**"	has the meaning given in paragraph 7.3.3(a) of Schedule 2.4 *(Security Management*);
"**Wider Information Management System**"	means those information assets, ICT systems and/or Sites which will be used by the Supplier and/or its Subcontractors to Process Authority Data which have not been determined by the Authority 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;
"**Working Day**"	means any day other than a Saturday, Sunday or public holiday in England and Wales.

SCHEDULE 2.1

SERVICES DESCRIPTION

Issue No:	Summary of Change:
V0.1	Version for issue with ITT.

I. **DEFINITIONS**

i. In this Schedule, the definitions set out in Schedule 1 shall apply.

1. **INTRODUCTION**

1.1 As the Authority and its organisations, the Service Recipients, have come together over recent years, our individual organisations have each brought their own local commercial processes and systems. The Authority is bringing these into alignment with the Government Commercial Operating Standards (GCOS). “Project Victory” is been tasked with delivery of a suite of commercial systems which:

1.1.1 Work well for all Service Recipients, and align with GCOS requirements;

1.1.2 Facilitate more strategic procurement activities such as commercial and financial modelling, effective category management, market and supplier analysis and management, and, optionally, supplier relationship management;

1.1.3 Shift the NDA and its subsidiaries from manual data collection, manipulation and reporting to automated solutions;

1.1.4 Improve data integrity, and compliance with data standards;

1.1.5 Improve the ability to share and obtain information from/with other systems, particularly Enterprise Resource Planning (ERP) systems;

1.1.6 Enhance the ability to share information across the Service Recipients, and also into and out of central government;

1.1.7 Dovetail with central government systems, such as the Contracts and Spend Insight Engine (CaSIE), without the need for 'double keying' or manual intervention to upload data; and

1.1.8 Enable baselining and measurement of government targets for supply chain spend, such as through small and medium-sized enterprises (SMEs).

2. OPERATIONAL SERVICES

2.1 In addition to Schedule 4.1 (*Supplier Solution*), the Supplier shall provide the following Operational Services:-

2.1.1 The provision and maintenance of operational software and interfaces which meet the functional requirements for the System set out Volume 3 of the ITT; the Interfaces Overview Document; and the System Descriptor as included in Volume 7 of the ITT, as detailed in Appendix 1;

2.1.2 The provision of supported data migration to import legacy supplier data to the system, in accordance with Schedule 6.1 (*Implementation Plan*);

2.1.3 The provision of training and training materials in accordance with Schedule 6.1 (*Implementation Plan*);

2.1.4 The provision of an escalation route for unresolved issues (e.g., a Supplier Account Manager), or for issues raised out-of-hours in a critical situation.

2.1.5 The provision of performance reporting in accordance with the requirements of Schedule 2.2 (*Performance Levels*); and

2.1.6 The provision of software patches and developments in accordance with an agreed schedule to ensure the software is secure and stable, and to provide enhancements to functionality as agreed with the Supplier Group, as defined in Schedule 8.1 (*Governance*).

APPENDIX 1

DETAILED REQUIREMENTS

A	**General System Requirements/User experience/Master Data Management**
A1	**The system configuration meets the criteria below**
A1.01	The system must be available 99.9% of the time following award, and any downtime for maintenance must be agreed by Contracting Authority in advance, as per the Service Levels Agreements and Service Credits policy. The Contractor will supply evidence of maintained business continuity and disaster recovery plans, which will include the target recovery time of 2 hours in the event of system failure.
A1.02	The system is accessible from all common web browsers on Windows platforms via a secure web address, with no requirement for software/code/ActiveX controls to be downloaded to a user or supplier computer. The system should be able to operate effectively with a standard broadband connection (8MB down, 2MB up). The system will be built on an industry-recognised robust coding platform using encryption at rest.
A1.03	The system must be accessible for users who use assistive technology to overcome an impairment, and must conform to the Public Sector Bodies Accessibility Regulations 2018
A1.04	User access to the system is controlled via a role-based or user group profile mechanism so that the access of all users in a group can be maintained and modified as requirements develop. Access can be controlled by module, category, NDA subsidiary, department etc.

A1.05	Designated super users can assign users to roles/profiles and customise individual access.
A1.06	Helpdesk support is to be provided by the Contractor with cover from 0830 – 1700 Monday to Friday GMT (Greenwich Mean Time) as a minimum. This will offer two key services: - First-line support to suppliers having difficulty with using the system (referring issues related to individual projects to super-users) - Second-line support for issues escalated by super-users across the NDA group Helpdesk will provide access via phone, email, or system messaging. The content and associated metadata of email and system messaging communications will be retained for the duration of the contract, and accessible on demand by NDA group contract manager.
A1.07	User password structure is adapted to meet NDA organisational standard requirements, which follow National Cyber Security Centre guidelines
A1.08	Users can carry out self-service password reset via their official email address. Lost usernames would require helpdesk support and confirmation.
A1.09	Designated super-users can assign new users to the system

A2	**The system configuration meets the criteria below**
A2.01	Data are maintained at high quality and data entry is eased by, for example: - Standard formatting across the system, including UK style for dates, currency etc. - Use of drop-down/checkboxes/radio buttons to limit free text entry wherever possible - Fields can be marked as mandatory or optional for entry - Free-text fields have character limits stated - System names use standard UK procurement terms as defined in the Public Contracts Regulations 2015

	- Support for the relevant standard and NDA-specific fields set out in the attached data dictionary Data provided by the Contractor in the system is refreshed regularly to ensure it is up to date
A2.02	Data entered includes unique identifiers for contracting entities (including companies, charities, joint ventures), for instance company/charity registration ID's or DUNS numbers, to enable consistent master data quality
A2.03	The system can store documents and media in a range of common office formats, for example, Microsoft, Open Office, Adobe PDF, common formats for graphics, etc.

A3	**The system configuration meets the criteria below**
A3.01	Each NDA business can distinguish its own data on the system, including: • Suppliers and associated profiles • Supply chain map • Supplier communication exchanges • Procurement categories
A3.02	Pan-NDA data are available to all users, including: • Suppliers and associated profiles • Supply chain map, aggregated from the individual NDA business' supply chain maps • Risk indices and associated weightings • Business continuity plans, documentation, and scores • Mitigation action events

A4	**The system configuration meets the criteria below**

A4.01	The Contractor maintains and communicates to the system owners a forward view of system developments and releases. Maintenance/upgrades come with full user documentation.
A4.02	Major system developments are available to trial ahead of full release, and a clear channel for provision of feedback to the Contractor by NDA super users is provided
A4.03	Following release of the next iteration of the system, the preceding iteration is held as a back-up for 90 days to avoid loss of service if the new release is determined by NDA to be unsatisfactory
A4.04	The Contractor operates a process to ensure continuous improvement of its service to NDA

B	**Supply chain mapping and supplier engagement**
B1	**The system configuration meets the criteria below**
B1.01	The system allows NDA to create a map of its supply chain to at least four tiers down. The system can create visual maps by category of spend, NDA group business, part, product, programme of work, and the global geographical location of the supplier (i.e. the location of the source of supplies). The supply chain map shall contain access to the supplier's information and have the capability to view both as a network diagram and on a geographical map. Mapping will be geocoded via longitude & latitude, or post code
B1.02	The system hosts supply chain mapping data on up to 3000 Tier 1 suppliers. Tier 1 suppliers are added to the system on a self-serve basis as and when required by NDA. Suppliers at and below Tier 2 are added to the system at no charge. There is no cap on the number of suppliers at Tier 2 and below that can be added to the system.
B1.03	Supplier data are added to the system via completion of a survey. The survey functionality allows any number of surveys to be generated by NDA users on a self-serve basis, with technical assistance provided by the Contractor where requested.

	The survey functionality provides industry-standard survey functions, including: • Multiple data input formats – character-limited textual input, non-character limited textual input, sequential and non-sequential dropdown menus, radio entry, tick-box, single and multiple-choice matrices, tooltips • One or more pages • Covering, header and footer text inputted by NDA user who created the survey Standard and NDA-specific survey templates can be saved in the system for repeated later use. The results of individual, and aggregates of, surveys can be downloaded in spreadsheet format for off-system interrogation The system supports customisable surveys to suppliers, for example, to provide input to business continuity plans, sub-tier mapping, quality management, physical security, cyber security, and certifications
B1.04	Supplier data that is inputted is to include at least but not limited to: • Company details – name, registered address, company registration number, DUNS • Contacts (at least one named contact required) – contact name, postal address and post code, telephone number, and email address • Site list – postal address and post code, contact name, telephone number (per site) • Parts and programmes – items provided to deliver services to NDA group • Sub-tier suppliers – name, registered address, company registration number, DUNS, relation to operations for NDA • Sub-tier sites – postal address and post code, contact name, telephone number (per site) • Sub-tier supplier parts and programmes – items provided to deliver services to NDA group (supplemented by data input from sub-tier suppliers where required) Built-in functionality prevents users and suppliers inputting data where mandatory fields have not been provided. The labelling of data as mandatory or non-mandatory can be changed on demand by request of NDA contract manager to the Contractor.
B1.05	The system enables suppliers to enter and manage their own data for supply chain mapping and survey responses. Supplier data input is facilitated through a secure portal provided by the Contractor. Suppliers can view their own data and enable alerts of any adverse indicators that may affect their operations. Where supplier data is already held in the system this is presented to them for verification and to ease data input. Ownership of data entered on the system by suppliers is retained by the supplier, to satisfy data protection requirements. Such data can be amended and deleted by the supplier at any time.

B1.06	The system enables designated NDA super-users to upload/enter details of suppliers. The system allows for the storage of information and documents within a supplier's record, and survey responses.
B1.07	The upload of supplier data includes a data normalisation process where variations of supplier identifier data (i.e., trading name, registered address, company registration, DUNS number) are aligned to a master record, to ensure there exists a single record for each entity
B1.08	The system provides suitable templates for suppliers to provide details of their business continuity plans and associated documentation via the system's survey functionality, supported by easily identifiable flags when this is required and/or absent.
B2	The system configuration meets the criteria below
B2.01	Geographic maps and associated data will be from a reputable source, and be accurate and updated in real time as underlying data are updated (i.e. by the Contractor's provider of geographic maps)
B2.02	Supplier ownership structures can be identified in supply chain maps
B2.03	Tags can be applied to individual and groups of suppliers. The name and visual display of tags can be customised to allow NDA to label suppliers according to current and future analytical requirements.
B2.04	Multiple data dimensions (i.e. category, tag, part, product, NDA group business, programme of work) can be applied to a supplier

B3	**The system configuration meets the criteria below**
B3.01	The system provides an in-flow of data on commodities chosen by NDA to be monitored. Data are at the global level as a minimum, and national wherever possible. Data covered include current and projected price per unit, current and projected demand, current and projected availability, and qualitative narrative of the data.

B3.02	Where commodities are identified as being used in the NDA group's supply chain, relevant data are presented to allow on-system analysis of impact to NDA group operations and providers in the supply chain. Wherever possible the in-flow of data on commodities is linked to parts and products included in the supply chain map and supplier data held in the system
B3.03	Maps of material flows across geography and between suppliers can be created, with data visualised both on geographic maps and in tables and graphs. The material flow data allows for entering of bills of materials data by designated NDA super users.
B3.04	The data on commodities applies machine learning functionalities so that the occurrence of certain events are flagged as potentially impacting upon the availability of certain commodities. However, at all times, commodity data is derived from robust and verifiable sources.
B4	The system configuration meets the criteria below
B4.01	Contract data can be assigned to suppliers included in the system. Contract data are inputted by the NDA, either manually or via interface from the Lot A system. Contract data will include header data like contract title, contract reference, end date, and spend category
B4.02	Contract data are visually represented on supply chain maps and relevant dashboards and reports in the system
B4.03	The system supports the simplified version of the United Nations Standard Products and Service Codes (UNSPSC) used in the NDA group, Standard Industrial Classification codes (SIC), the UK Government's Common Areas of Spend: Procurement taxonomy (CAS), and NDA group procurement categories to categorise procurement expenditure.
B4.04	NDA group sites can be included in the system so that relevant geographic mapping, alerts, risk indices, risk mitigation events, and business continuity scores can be assigned and connected to supply chain maps, geographic mapping, and incidents
B5	The system configuration meets the criteria below
B5.01	On each supplier's profile and in risk mitigation events a secure area for communication between NDA users and the supplier is provided
B5.02	The Contractor is unable to access data and correspondence shared in the communication area, to maintain confidentiality of discussions and documentation

C	Risk event monitoring
C1	**The system configuration meets the criteria below**
C1.01	The system provides warning, in advance wherever possible, of events that may impact the supply chain via alerts from a wide variety of sources, including the ability to monitor specific suppliers, geographic locations and industries. Configurable email alerts are automatically generated to users based on events configured within the system. The content of such emails can be configured by the Contractor after request by the NDA group contract manager to meet organisational requirements. Alerts can be configured to be distributed at different time frequencies, including instantly, daily, weekly, monthly, and quarterly
C1.02	Horizon scanning alerts are provided that include the ability to monitor specific suppliers, geographic locations, and industries. Alerts can be configured to search by supplier name, NDA group business, material and commodity name.
C1.03	Alerts contain recommendations for action based on the data held in the alert event, the NDA's supply chain data in the system, and other relevant contextual information. Alerts are subject to a robust quality assurance process, where data are verified via multiple sources wherever possible. The content of alerts is informed by the expertise of supply chain risk professionals.
C1.04	Suppliers to NDA whose data are loaded into the system receive alerts for risks that are assessed to affect them, virtue of geography or industry of operation
C2	The system configuration meets the criteria below
C2.01	The system provides for identification, categorisation, scoring, monitoring, and management of operational risks, including but not limited to: • Capacity constraints and pinch points • Supplier dependency, skills, equipment, or material shortages

	• Economic and financial risk identification, scoring, monitoring and management of risk in the supply chain e.g. supplier financial standing, currency fluctuations, shorting market, mergers and acquisitions, global linkage • Political, societal, technological, legal, and environmental risk The risk metrics are relevant to NDA operations and can be amended to ensure they are suitably rated.
C2.02	The system allows for the entering of custom supplier risk metrics by designated users across NDA group, for example quality and business continuity scores.
C2.03	The weighting of risk indices can be customised at an NDA business, industry, and supplier-specific, level by designated NDA super-users
C2.04	The nature of risk scores held in the system focus on either supply risk or health. Where third-party risk data are inputted the system ensures this focus is maintained, wherever required automatically reverting or converting the third-party indices to ensure this consistency is maintained.
C2.05	Risks are monitored and follow-on analysis is provided 24 hours a day, seven days a week, 365 days a year
C2.06	An explanation of the underlying source and methodology of indices and data are provided to users on a self-serve basis, ideally within the system interface
C2.07	The system could have media scrubbing functionality, including identification of adverse and obverse media coverage of suppliers to NDA group, quantification of the media coverage to identify any impacts on risk, and subsequent presentation of the media coverage including primary source and integration of data to relevant risk scores in the system
C3	The system configuration meets the criteria below
C3.01	The Contractor and/or sub-contractors can provide data on economic, financial, political, societal, technological, legal, and environmental risk. The data is robust, accurate, and derived from a reputable source(s). Sources of intelligence additional to those provided by the system contractor, to be used in the system, can be provided through third parties (Risk data feed providers). The system can integrate these data from external parties into relevant modules and areas of the system.

	These externally provided data can be facilitated through use of existing or new affiliate relationships between the system provider and data providers, and/or sub-contracted arrangements. Risk data could cover the following topics: • Natural hazards • Man-made hazards • Space hazards • Dual and multi-hazard incidents • Supply issues • Payment duration ('Prompt Payment') • Sustainability • Environmental quality • Climate change • Carbon emissions and reductions • Modern day slavery • Human rights and sanctions • Civil unrest • Corruption • Terrorism • Institutional stability • Migration • Infrastructure availability, quality, and developments • Educational attainment and quality • Business size (SME status) • Cyber security • Technological development • Regulatory control and compliance • Ethical procurement These data are applied in the system to one or more of the following: • Suppliers • Industries • Commodities • Geographies, including by locale/postal code wherever relevant

D	Risk analysis, management, and mitigation
D1	**The system configuration meets the criteria below**
D1.01	The internal system administrators can create, modify, and delete templates and process workflows as required, with a full audit trail maintained for the duration of the contract, and accessible on demand by NDA group contract manager.
D1.02	The system supports the preparation, approval, delivery, and monitoring of action plans for risk mitigation – shared between internal users and suppliers (with appropriate security controls over access).
D1.03	Both upon generation of an alert, and when manually created by designated NDA group users, a risk mitigation event is created where relevant information relating to the alert is brought together. The trigger or threshold for the creation of a risk event can be configured by the Contractor together with the NDA contract manager. Suppliers who receive a risk alert in the system are automatically included in the risk mitigation event and receive an email notification of the alert and their inclusion in the risk mitigation event. The status of each risk mitigation event is clearly displayed in the system and on the profile page of the event. The status will be Open, Closed, or Pending. Closed risk mitigation events are retained and accessible to users for future reference, and in any event are deleted only at the express request of an NDA super user. This includes documentation and correspondence shared in the risk mitigation event area of the system.
D2	The system configuration meets the criteria below
D2.01	The system enables the simulation of ‘what-if’ scenarios to support effective risk management
D2.02	The scenario simulation section allows analysis across geography, industry, individual and groups of suppliers, commodity, parts and products, NDA group business, and programme of work.
D2.03	Scenario simulation by geography is facilitated by user input of polygonal visual overlays
E	Reporting and data transfer

E1	**The system configuration meets the criteria below**
E1.01	Dashboards are provided that enable quick and easy to read analysis of the target data, including but not limited to: • Individual and groups of suppliers • Risk scores and averages by supplier, geography, industry, NDA business, procurement category, programme of work, and NDA business • Risk mitigation events – status, criticality, ownership • Supplier data input progress tracking • Ongoing supplier interaction including surveys Users can configure their own personal dashboard. Filters applied to the personal dashboards are retained as users log on an off the system. Custom dashboards can be created by the Contractor on request by the NDA contract manager.
E1.02	The system includes a suite of flexible operational reports to view the overall supply chain status, risk etc and to identify 'hotspots' where risk needs to be addressed, including geographically. Reports enable the download of data in bulk without request to the Contractor.
E2	The system configuration meets the criteria below
E2.01	The system supports bulk import of data independently of the Contractor at no charge, administered through a visually accessible and clean-designed interface. The progress of bulk input activities is clearly displayed in the system. Bulk input activities follow a set, clear, visible and logical process.
E2.02	Data upload activities are completed within two business days after initiation by NDA or the Contractor.
E2.03	Record of data input activities is retained in the system for the duration of the contract, and clearly indicate the outcome (successful, unsuccessful, pending) of each input record.
E2.04	The system allows the bulk export of data independently of the Contractor in spreadsheet format, accessible via common computer-based office software (e.g., Microsoft Excel, LibreOffice Calc, Google Sheets). This includes ability to export individual tables of data that are visualised in the system, alongside export of data models and tables that underlie the information shown in the system.

	This includes data on: • Suppliers • Commodities • Risk indices (individual and aggregated) • Contracts • Business continuity • Risk mitigation events • Supply chain maps
E2.05	Data on suppliers, supply chain mapping, workflow, scenario simulation, business continuity, and risk alerts, can be exported in a text and image publishing format accessible via common computer-based office software (e.g. Adobe PDF, Microsoft Word). This also includes ability to use internet browser capabilities to 'print' screens as displayed on the user's device.
F	**Internal NDA and external system interfaces meet the criteria below:**
F1	**Please refer to Volume 5 – Interfaces Overview Lot D for further detail on the interfaces between systems in Project Victory.**
F1.01	The system interfaces (automated or manually) with contract management systems (Project Victory Lot A) to receive updates to contract and supplier master data
F1.02	The system interfaces with the Dun & Bradstreet system provided to NDA through Project Victory Lot B. This includes transfer of supplier header, financial, payment and sanction data via the Automated Programme Interface (API) provided to NDA by Dun & Bradstreet. The data that are required to be transferred will be nominated to the Contractor by the NDA contract manager. Data transferred via API are applied to suppliers operating at all tiers mapped in the NDA system.
F1.03	The system interfaces with the RapidRatings system provided to NDA through Project Victory Lot B. This includes transfer of supplier header and financial data via the API provided to NDA by RapidRatings. The data that are required to be transferred will be nominated to the Contractor by the NDA contract manager. Data transferred via API are applied to suppliers operating at all tiers mapped in the NDA system.

F1.04	The system shares data via API to the analytics platform (Project Victory Lot E) to provide linked comprehensive dashboarding of supply chain spend and risk by category/sub-category/product, organisation, department, contract etc., and for reporting at an organisational and group-wide level
G	**Account management**
G1	**The system configuration meets the criteria below:**
G1.01	The Contractor provides training on a 'train the trainer' basis to all users, to be delivered remotely. The Contractor provides training to all NDA group users on an annual basis, delivered remotely and which is recorded for later reference and provided to the NDA contract manager at no additional charge. The Contractor supports training with a range of online help and other materials including videos. The Contractor provides training to suppliers on entering and managing their data in the system, and on the alerts and risk mitigation event functionalities.
G1.02	The Contractor provides a clearly identified process for escalating cases where further assistance, beyond that provided in user manuals and training sessions, for users or suppliers is required.
G1.03	In the event of system downtime/service degradation, email notification to the entire user base by the Contractor.
G1.04	The Contractor provides full delivery support to enable effective use of the system, with a project plan for on-boarding following contract award and ongoing business as usual support. An implementation plan will be provided by the Contractor through the tender process and enacted after contract award.
G1.05	Scheduled contract management meetings will take place at least quarterly between nominated representatives of the Contractor (at a minimum the Contractor's account manager for NDA), the NDA contract manager, and other NDA group colleagues requested to join by the NDA contract manager. The agenda for such meetings will cover at least: • Review of current service use • Review of live and closed issues

	• Forthcoming and planned system release and functionality developments • Review of Contractor performance vis-à-vis the contract terms and conditions (i.e., SLAs, KPIs) Management information are available on-demand by NDA contract manager to the Contractor, and will include as a minimum information on: • User access • Number of users registered • Number of suppliers included in the system (overall, and disaggregated by NDA group business) • Number of risk mitigation events, with status (open, close) and associated dates included

PART 2: SOCIAL VALUE

This Social Value section evaluates the Bidder's understanding of, and approach to, delivering social value through its provision of services to NDA through this contract.
The Bidder is requested to provide a suitable response to each of these requirements.

SV	**Social Value – Training and Upskilling**
SV-A	**Detail how your organisation's (and any sub-contractor's) approach to recruiting and training early talent will be undertaken when delivering this contract. Bidders should consider Themes 1, 2 and 4 of The Social Value Model when preparing their response (see** Procurement Policy Note 06/20 – taking account of social value in the award of central government contracts - GOV.UK (www.gov.uk)**).**

	Note that images can be included in your response and do not count towards the word count; images of elements not related to this question will count towards the word count.
SV	**Social Value – Health and Wellbeing**
SV-B	**Detail the measures you will take to maintain, and where required improve, the level of health and wellbeing of staff working on the provision of this contract. Bidders should consider Theme 5 of The Social Value Model when preparing their response (see** Procurement Policy Note 06/20 – taking account of social value in the award of central government contracts - GOV.UK (www.gov.uk)**)** **Note that images can be included in your response and do not count towards the word count; images of elements not related to this question will count towards the word count.**

TX.01	Data is maintained at high quality and data entry is eased by: • Standard formatting across the system, including UK style for dates, currency etc. • Use of drop-down/checked boxes/radio buttons to limit free text entry wherever possible • Fields can be marked as mandatory or optional for entry by system administrators • Free-text fields have character limits stated
TX.02	The system provides users with both general and context-sensitive help information to support both initial familiarisation and to lead users through a process journey. Video material, or similar, is available to guide users, including suppliers.
TX.03	The system is straightforward to access and navigate, with a clean, clear, modern, and user-intuitive design throughout
TX.04	The system includes a suite of flexible operational reports to view the overall supply chain status, risk etc and to identify 'hotspots' where risk needs to be addressed, including geographically. Reports enable the download of data in bulk without request to the Contractor.
TX.05	The system allows the bulk export of data independently of the Contractor in spreadsheet format, accessible via common computer-based office software (e.g., Microsoft Excel, LibreOffice Calc, Google Sheets). This includes ability to export individual tables of data that are visualised in the system, alongside export of data models and tables that underlie the information shown in the system.

	This includes data on: • Suppliers • Commodities • Risk indices (individual and aggregated) • Contracts • Business continuity • Risk mitigation events • Supply chain maps
TX.06	Data on suppliers, supply chain mapping, workflow, scenario simulation, business continuity, and risk alerts, can be exported in a text and image publishing format accessible via common computer-based office software (e.g. Adobe PDF, Microsoft Word). This also includes ability to use internet browser capabilities to 'print' screens as displayed on the user's device.

TA.01	The system allows NDA to create a map of its supply chain to at least four tiers down. The system can create visual maps by category of spend, NDA group business, part, product, programme of work, and the global geographical location of the supplier (i.e. the location of the source of supplies).
TA.02	Supplier data are added to the system via completion of a survey. The survey functionality provides industry-standard survey functions, including: • Multiple data input formats – character-limited textual input, non-character limited textual input, sequential and non-sequential dropdown menus, radio entry, tick-box, single and multiple-choice matrices, tooltips • One or more pages • Covering, header and footer text inputted by NDA user who created the survey Standard and NDA-specific survey templates can be saved in the system for repeated later use.
TA.03	Supplier data that is inputted is to include at least: • Company details – name, registered address, company registration number, DUNS • Contacts (at least one named contact required) – contact name, postal address and post code, telephone number, and email address • Site list – postal address and post code, contact name, telephone number (per site) • Parts and programmes – items provided to deliver services to NDA group

	• Sub-tier suppliers – name, registered address, company registration number, DUNS, relation to operations for NDA • Sub-tier sites – postal address and post code, contact name, telephone number (per site) • Sub-tier supplier parts and programmes – items provided to deliver services to NDA group (supplemented by data input from sub-tier suppliers where required)
TA.04	The upload of supplier data includes a data normalisation process where variations of supplier identifier data (i.e., trading name, registered address, company registration, DUNS number) are aligned to a master record, to ensure there exists a single record for each entity.

TB.01	The system provides warning, in advance wherever possible, of events that may impact the supply chain via alerts from a wide variety of sources, including the ability to monitor specific suppliers, geographic locations and industries.
TB.02	The system provides for identification, categorisation, scoring, monitoring, and management of operational risks, including but not limited to: • Capacity constraints and pinch points • Supplier dependency, skills, equipment, or material shortages • Economic and financial risk identification, scoring, monitoring and management of risk in the supply chain e.g. supplier financial standing, currency fluctuations, shorting market, mergers and acquisitions, global linkage • Political, societal, technological, legal, and environmental risk The risk metrics are relevant to NDA operations and can be amended to ensure they are suitably rated.
TB.03	On each supplier's profile and in risk mitigation events a secure area for communication between NDA users and the supplier is provided
TB.04	The Contractor and/or sub-contractors can provide data on economic, financial, political, societal, technological, legal, and environmental risk. The data is robust, accurate, and derived from a reputable source(s). These data are applied in the system to one or more of the following: • Suppliers • Industries • Commodities • Geographies, including by locale/postal code wherever relevant

	Sources of intelligence additional to those provided by the system contractor, to be used in the system, can be provided through third parties (Risk data feed providers). The system can integrate these data from external parties into relevant modules and areas of the system.
TB.05	The system allows for the entering of custom supplier risk metrics by designated users across NDA group, for example quality and business continuity scores.
TB.06	The weighting of risk indices can be customised at an NDA business, industry, and supplier-specific, level by designated NDA super-users
TB.07	The internal system administrators can create, modify, and delete templates and process workflows as required
TB.08	Both upon generation of an alert, and when manually created by designated NDA group users, a risk mitigation event is created where relevant information relating to the alert is brought together. Suppliers who receive a risk alert in the system are automatically included in the risk mitigation event and receive an email notification of the alert and their inclusion in the risk mitigation event.

THE SYSTEM

This section describes the high-level requirement for the system and provides further context. The system is intended to provide the tools to facilitate the management of commercial risk.

NDA is open to proposals that include elements of the system being provided by third parties through a sub-contractor arrangement.

Commercial Risk Management

The system will

- Support identification of at least the first three tiers of our supply chain (some contracts will have deeper supply chains) for a core set of our contracts and enable the NDA group to identify, assess, mitigate and monitor risks within that scope for each category/sub-category/critical product, department and NDA group business
- Use financial and performance intelligence to identify suppliers at risk of business failure, alerting users of changes so that action can be taken
- Support the effective management of business continuity in relation to the supply chain
- Enable identification of over-reliance on single or multiple suppliers

- Enable the NDA group to map supply lines by each supplier's geographical locations[1] and detail risk exposure to programmes and spend categories including, for example, metrics on geopolitical, macroeconomic and natural hazards
- Enable the NDA group to map where SMEs or Social Enterprises are operating in supply chains and spend categories
- Enable the NDA group to create a live picture of the NDA group's supply chain where key Government policy agenda matters are significant, such as the potential for human rights abuse, good employment practice issues, sustainability and the environment etc. to develop suitable action plans
- Enable supply chain risk mitigation within the system, including collaboration between teams

Supply Chain Mapping
The system will

- Facilitate more strategic management of NDA group third party spend, creating a visual picture of supply chains mapped to categories and NDA businesses.
- Enable more effective market management by supporting the mapping of procurement pipeline data on to a map of current live contracts and comparing that to market size and value (either directly or by providing data to the Lot E analytics system for mapping alongside data from the Lot A pipeline management module).

The projected number of suppliers to be loaded into the system are:

- Projected number of Tier 1 suppliers in the system - initial load (480), Year 1 (up to 600), Year 2 (up to 1000), from Year 3 onwards (up to 1600)
- Projected number of sub-tier (Tier 2 and below) suppliers - initial load (430), from Year 1 onwards (1000), with ability to purchase additional if required and as stated in the Additional Optional Costs section of Volume 4 – Pricing Matrix

Supplier data are inputted by NDA and/or the Tier 1 or sub-tier suppliers; the system provider is not expected to input these data, unless explicitly requested by NDA and as costed under Additional Optional Costs in Volume 4 – Pricing Matrix.

Illustrative Examples

Example 1: Supplier Financial Risk

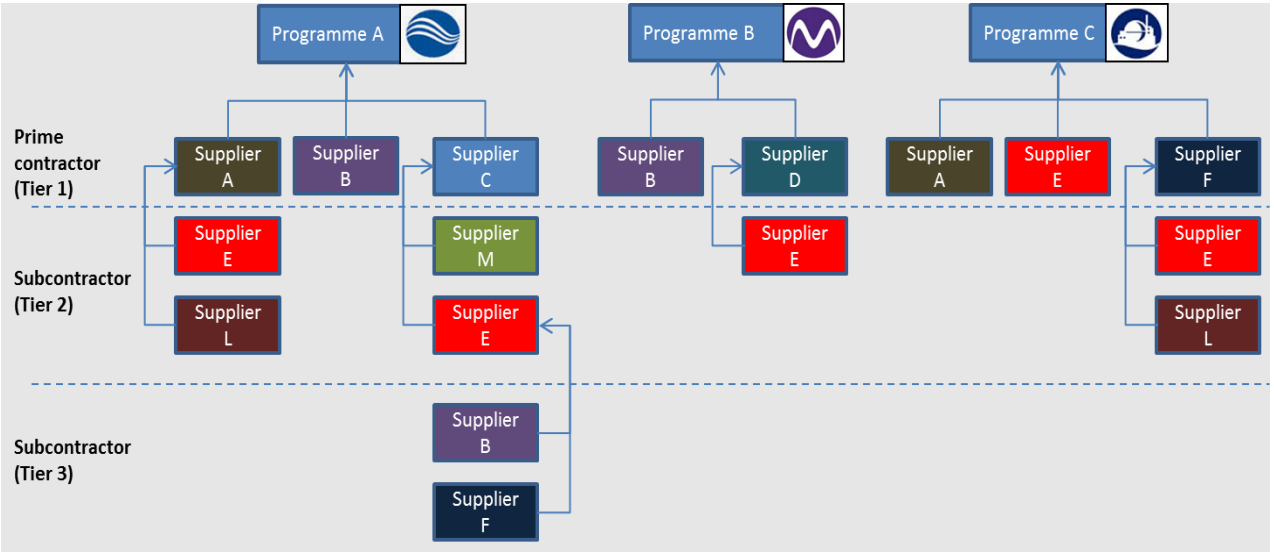
[1] i.e., the location of the source of supplies

The diagram below shows a mock-up of three separate NDA group programmes of work: Programme A is being led by Sellafield, Programme B by Magnox and Programme C by DSRL. At prime contractor level, just one programme – C – appears to be using Supplier E. Based on this visibility, the NDA group might assume it had relatively low exposure to Supplier E (shown in red), i.e., if the supplier were to enter financial distress, only 1 element of programme C at DSRL would be at risk.

However, by mapping further down the supply chain for each programme, we can see that Supplier E actually appears in a further four supply chains, which are spread across all three programmes and NDA businesses. The failure of Supplier E therefore has a much wider impact than Programme C at DSRL. If the NDA group knows this in advance of the supplier failure, it can put commercial contingency plans in place and monitor the supplier more closely.

The Supply Chain Risk Management System will enable the NDA group to identify the aggregate supply chain risk. It will take contract line data from the Lot A Contracts Register for the in-scope Tier 1 contracts and organise contracts on to a map according to their associated programme of decommissioning. Tier 2 and Tier 3 contracts are manually populated by either NDA group or procurement teams, using the information provided by the supplier as part of the bidding process.

The Supply Chain Risk Management System will also import data from the Lot B Market Intelligence Systems, e.g. financial risk ratings, and incorporate them into the map according to supplier of each contract.

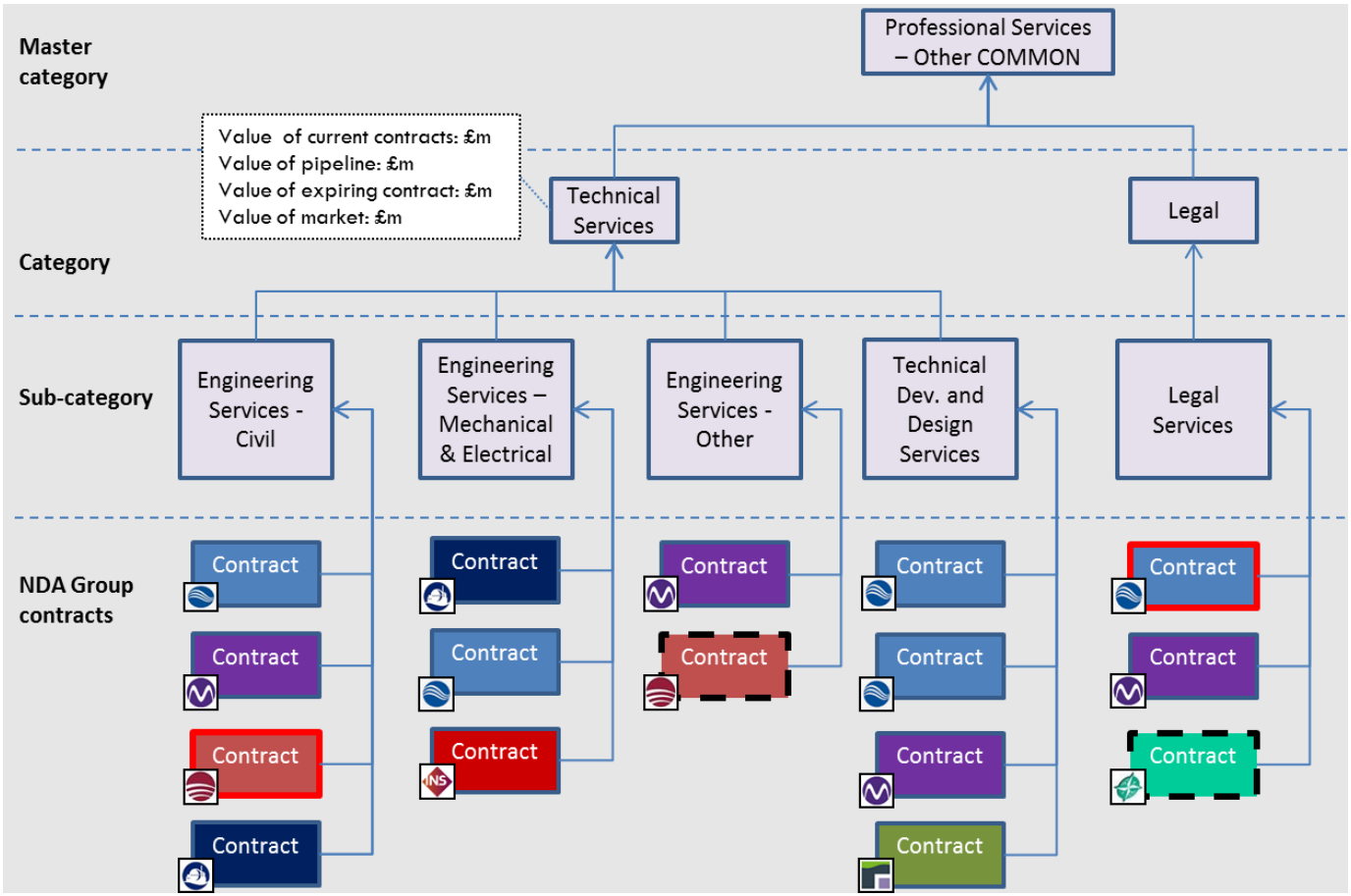


Example 2: Market Capacity and Category Management

The diagram below shows a mock-up of NDA group live contracts and pipeline contracts mapped by the government categories of spend (Common areas of spend: procurement). The red framed contract boxes show contracts that are expiring; the dashed framed contract boxes show contracts that are in the pipeline. The shading in the boxes represents different NDA group organisations e.g. purple boxes are Magnox.

Mapping contracts in this way provides a visual picture of the contract landscape to support category management and market management. It can be used to see opportunities for collaboration, see where there might be capacity constraints in the market, see what leverage the NDA group has in the market etc.

The system should support this locally and be able to provide data to the Lot E analytics system for visualisation alongside data from the other systems in the landscape.


Master category
Professional Services – Other COMMON
Value of current contracts: £m
Value of pipeline: £m
Value of expiring contract: £m
Value of market: £m
Technical Services
Legal
Category
Sub-category
Engineering Services - Civil
Engineering Services – Mechanical & Electrical
Engineering Services - Other
Technical Dev. and Design Services
Legal Services
NDA Group contracts
Contract

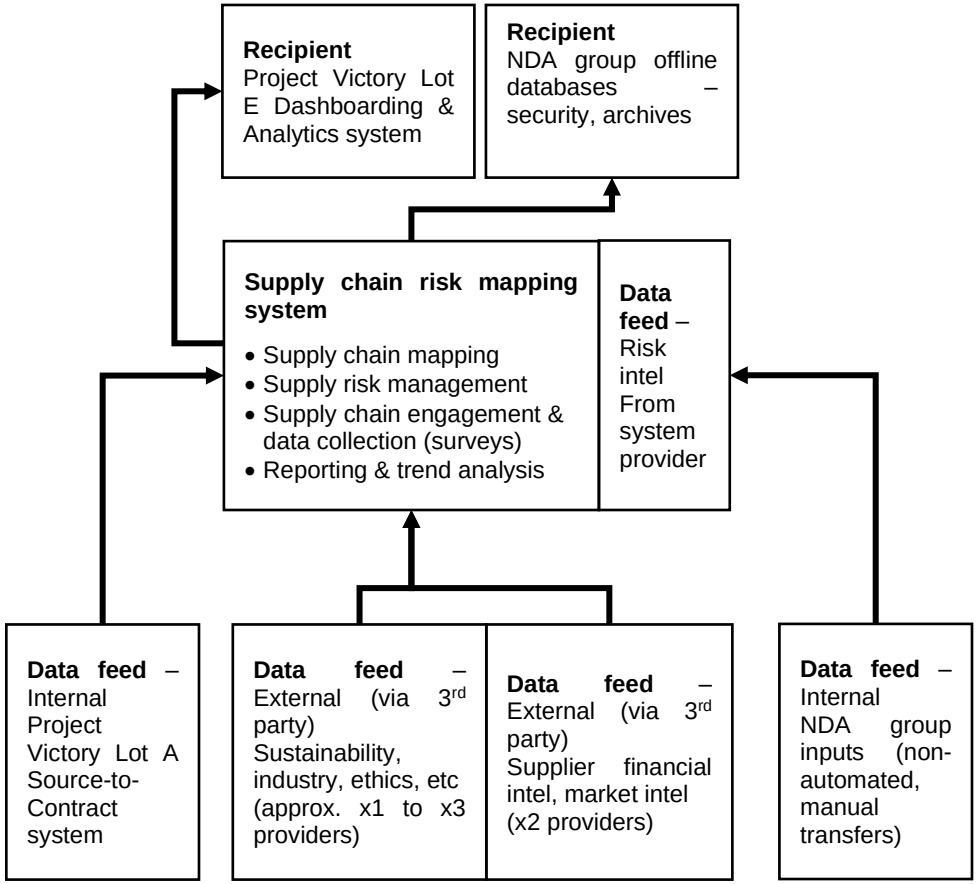
Associated supply chain intelligence:
The system will receive multiple data feeds that allows it to analyse and visualise information on suppliers and markets related to areas of regulation and compliance for the NDA group.

These data can be provided by the System contractor, or via input from third-party Data Feed providers.

Regardless of source, the data will provide UK-focussed insight on at least the following topics:

- Corporate Social Responsibility (CSR)
- Sustainability
- Modern-day slavery
- Data protection and cyber security
- Supplier financial health
- Convictions, charges and adverse exposure of businesses, and their officers

Additional topics can be proposed by the System contractor.



See Volume 5 – Interfaces Overview Lot D for further detail on the required risk data interfaces.

The system will be structured so that supply chain maps for individual NDA businesses can be created and viewed both standalone and integrated into a pan-NDA group perspective. The diagram below indicates this set-up.

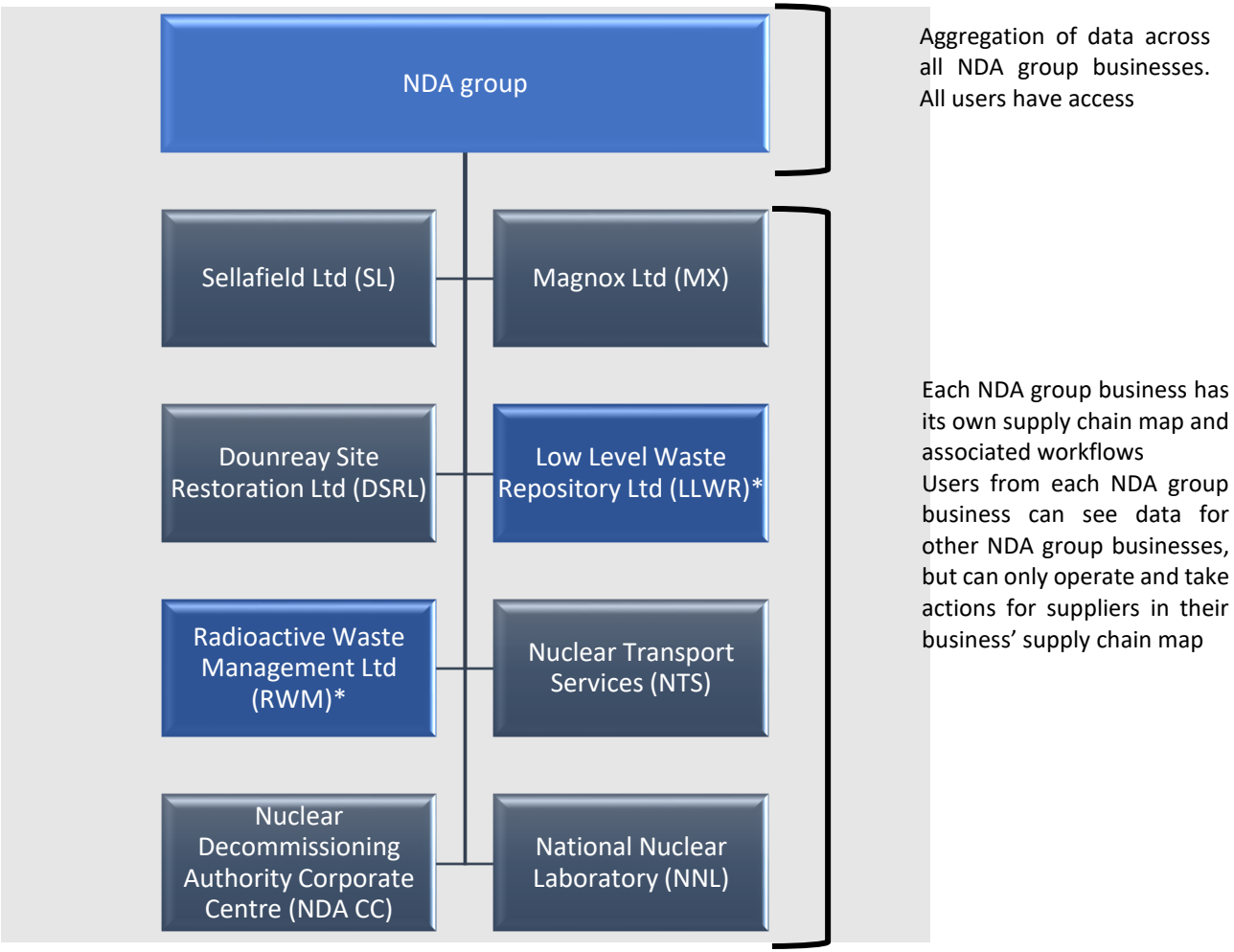


Figure 3 NDA group businesses, structured as required in the system

* RWM and LLWR are due to merge into a single Waste division in 2022, at present both will still require separate identifiers in the system

3.4 Reports and interfaces

The system will provide analysis of supply chains and enable operational reporting for commercial, category and contract managers, and management level reporting for all NDA group businesses.

It will also support the export and import of data, and interfacing via API with the main contract management system (Lot A) to enable the master contract register to provide details of new contracts.

The system will have the ability to link via API to the analytics platform (Lot E) for performance reports and dashboards.

See Volume 5 – Interfaces Overview Lot D for further detail on the required reporting interfaces.

SCHEDULE 2.2

PERFORMANCE LEVELS

Issue No:	Summary of Change:
V0.1	Version for issue with ITT

I. DEFINITIONS

ii. In this Schedule, the definitions set out in Schedule 1 shall apply.

PART 1

PERFORMANCE INDICATORS AND SERVICE CREDITS

1. KEY PERFORMANCE INDICATORS

1.1 0 sets out the Key Performance Indicators which the Parties have agreed shall be used to measure the performance of the Services by the Supplier.

1.2 The Supplier shall monitor its performance against each Key Performance Indicator and shall send the Authority a report detailing the level of performance actually achieved in accordance with Part 2.

1.3 Service Points, and therefore Service Credits, shall accrue for any KPI Failure and shall be calculated every three months (the 'measurement period'), in accordance with paragraphs 2, 3 and 5.

2. **SERVICE POINTS**

2.1 If the level of performance of the Supplier during a Service Period achieves the Target Performance Level in respect of a Key Performance Indicator, no Service Points shall accrue to the Supplier in respect of that Key Performance Indicator.

2.2 If the level of performance of the Supplier during a Service Period is below the Target Performance Level in respect of a Key Performance Indicator, Service Points shall accrue to the Supplier in respect of that Key Performance Indicator as set out in paragraph 2.3.

2.3 The number of Service Points that shall accrue to the Supplier in respect of a KPI Failure shall be the applicable number as set out in 0 depending on whether the KPI Failure is a Minor KPI Failure, or a Serious KPI Failure, unless the KPI Failure is a Repeat KPI Failure when the provisions of paragraph 3.2 shall apply.

3. **REPEAT KPI FAILURES AND RELATED KPI FAILURES**

Repeat KPI Failures

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

3.2 The number of Service Points that shall accrue to the Supplier in respect of a KPI Failure that is a Repeat KPI Failure shall be calculated as follows:-

SP = P x 2

where:-

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

P = the applicable number of Service Points for that KPI Failure as set out in 0 depending on whether the Repeat KPI Failure is a Minor KPI Failure, a Serious KPI Failure, or a failure to meet the KPI Service Threshold.

Worked example based on the following Service Points regime for Service Availability

Service Availability Severity Levels		**Service Points**
Target Performance Level	99%	0
Minor KPI Failure	98.0% - 98.9%	1
Serious KPI Failure	96.0% - 97.9%	2
KPI Service Threshold	Below 96%	3

Example 1

If the Supplier achieves Service Availability of 98.5% in a given Measurement Period, it will incur a Minor KPI Failure for Service Availability in that Measurement Period and accordingly accrue 1 Service Point. If, in the next Measurement Period, it achieves Service Availability of 96.5%, it will incur a Serious KPI Failure and accordingly accrue 3 Service Points, but as the failure is a Repeat Failure, this amount is doubled and so the Supplier will incur 6 Service Points for the failure (ie SP = 3 x 2). If in the next Measurement Period it achieves Service Availability of 96.5%, the Supplier will again incur 6 Service Points.

Example 2

If the Supplier achieves Service Availability of 96.5% in a given Measurement Period, it will incur a Serious KPI Failure for Service Availability in that Measurement Period and accordingly accrue 3 Service Points. If, in the next Measurement Period, it achieves Service Availability of 98.5%, it will incur a Minor KPI Failure and accordingly accrue 1 Service Point, but as the failure is a Repeat Failure, this amount is doubled and so the Supplier will incur 2 Service Points for the failure (ie SP = 1 x 2). If in the next Measurement Period it achieves Service Availability of 96.5%, the Supplier will incur 6 Service Points.

Related KPI Failures

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

4. PERMITTED MAINTENANCE

The Supplier shall notify the Authority in writing of all planned Service Downtime for Permitted Maintenance.

5. SERVICE CREDITS

5.1 Schedule 7.1 (*Charges and Invoicing*) sets out the mechanism by which Service Points shall be converted into Service Credits.

5.2 The Authority shall use the Performance Monitoring Reports provided pursuant to Part 2, among other things, to verify the calculation and accuracy of the Service Credits (if any) applicable to each Service Period.

PART 2

PERFORMANCE MONITORING

1. PERFORMANCE MONITORING AND PERFORMANCE REVIEW

1.1 Within ten (10) Working Days of the end of each Service Period, the Supplier shall provide:-

1.1.1 a report to the Authority Representative which summarises the performance by the Supplier against each of the Key Performance Indicators as more particularly described in paragraph 1.2 and provides the underlying data that supports this (the "**Performance Monitoring Report**").

Performance Monitoring Report

1.2 The Performance Monitoring Report shall be in such format as agreed between the Parties from time to time and contain, as a minimum, the following information:-

Information in respect of the Service Period just ended

1.2.1 for each Key Performance Indicator, the actual performance achieved over the Service Period, and that achieved over the previous three (3) Service Periods and the underlying data that supports such performance;

1.2.2 a summary of all Performance Failures that occurred during the Service Period and the supporting information relating to the cause of any such Performance Failures;

1.2.3 the severity level of each KPI Failure which occurred during the Service Period and whether each KPI Failure which occurred during the Service Period fell below the KPI Service Threshold;

1.2.4 which Performance Failures remain outstanding and progress in resolving them;

1.2.5 for any Material KPI Failures occurring during the Service Period, the cause of the relevant KPI Failure and the action being taken to reduce the likelihood of recurrence;

1.2.6 the status of any outstanding Rectification Plan processes, including:-

(a) whether or not a Rectification Plan has been agreed; and

(b) where a Rectification Plan has been agreed, a summary of the Supplier's progress in implementing that Rectification Plan;

1.2.7 for any Repeat Failures, actions taken to resolve the underlying cause and prevent recurrence;

1.2.8 the number of Service Points awarded in respect of each KPI Failure;

1.2.9 the Service Points to be applied, indicating the KPI Failure(s) to which the Service Points relate;

1.2.10 the conduct and performance of any agreed periodic tests that have occurred, such as the annual failover test of the Service Continuity Plan and confirmation of any follow on actions or dates of re-testing to achieve compliance;

1.2.11 relevant particulars of any aspects of the Supplier's performance which fail to meet the requirements of this Agreement;

1.2.12 such other details as the Authority may reasonably require from time to time;

Information in respect of previous Service Periods

1.2.13 a rolling total of the number of Performance Failures that have occurred over the past six (6) Service Periods;

1.2.14 the amount of Service Credits that have been incurred by the Supplier over the past six (6) Service Periods;

1.2.15 the conduct and performance of any agreed periodic tests that have occurred in such Service Period such as the annual failover test of the Service Continuity Plan; and

Information in respect of the next Quarter

1.3 The Performance Monitoring Report shall be reviewed, and its contents agreed by the Parties at the next **"Performance Review Meeting"** held in accordance with paragraph 1.4.

1.4 The Parties shall attend meetings on a quarterly basis (unless otherwise agreed) to review the Performance Monitoring Reports. The Performance Review Meetings shall (unless otherwise agreed):-

1.4.1 take place within ten (10) Working Days of the Performance Monitoring Report being issued by the Supplier;

1.4.2 take place at such location and time (within normal business hours) as the Authority shall reasonably require (unless otherwise agreed in advance); and

1.4.3 be attended by the Supplier Representative and the Authority Representative.

1.5 The Authority shall be entitled to raise any additional questions and/or request any further information from the Supplier regarding any KPI Failure.

2. **PERFORMANCE RECORDS**

2.1 The Supplier shall keep appropriate documents and records (including Help Desk records, staff records, timesheets, training programmes, staff training records, goods received documentation, supplier accreditation records, complaints received etc) in relation to the Services being delivered. Without prejudice to the generality of the foregoing, the Supplier shall maintain accurate records of call histories for a minimum of twelve (12) months and provide prompt access to such records to the Authority upon the Authority's request. The records and documents of the Supplier shall be available for inspection by the Authority and/or its nominee at any time and the Authority and/or its nominee may make copies of any such records and documents.

2.2 In addition to the requirement in paragraph 2.1 to maintain appropriate documents and records, the Supplier shall provide to the Authority such supporting documentation as the Authority may reasonably require in order to verify the level of the performance of the Supplier both before and after each Operational Service Commencement Date and the calculations of the amount of Service Credits for any specified period.

2.3 The Supplier shall ensure that the Performance Monitoring Report, and any variations or amendments thereto, any reports and summaries produced in accordance with this Schedule and any other document or record reasonably required by the Authority are available to the Authority on-line and are capable of being printed.

3. **PERFORMANCE VERIFICATION**

The Authority reserves the right to verify the availability of the IT Environment and/or the Services and the Supplier's performance under this Agreement against the Key Performance Indicators including by sending test transactions through the IT Environment or otherwise.

APPENDIX 1

KEY PERFORMANCE INDICATORS

PART 1

KEY PERFORMANCE INDICATORS TABLES

The Key Performance Indicators that shall apply to the Operational Services and Optional Services are set out below:-

1. **KEY PERFORMANCE INDICATORS**

No	Key Performance Indicator Title	Definition	Frequency of Measurement	Severity Levels	Service Points
KPI 1	Service Availability	See paragraph 2 of	Monthly	Target Performance Level: Performance ≥99%	0

No	Key Performance Indicator Title	Definition	Frequency of Measurement	Severity Levels	Service Points
		Part 2 of this Appendix		Minor KPI Failure: 98.0% – 98.9% Serious KPI Failure: 96.0% – 97.9% KPI Service Threshold: below 96%	1 2 3
KPI 2	<Intentionally left blank>				
KPI 3	Average Fix Rate for Resolution of Logged Issues on First Response (during system up-time)	See paragraph 3 of Part 2 of this Appendix	Monthly	Target Performance Level: 75% Minor KPI Failure: 70-74.9% Serious KPI Failure: 60-69.9% KPI Service Threshold: <60%	0 1 2 3
KPI 4	Average Fix Rate for Resolution of Logged Issues Not Resolved on First Response (during system up-time) (during system up-time)	See paragraph 3 of Part 2 of this Appendix	Monthly	Target Performance Level: within two Working Days Minor KPI Failure: 1-2 Working Days Serious KPI Failure: 3-5 Working Days KPI Service Threshold: Over 5 Working Days	0 1 2 3

No	Key Performance Indicator Title	Definition	Frequency of Measurement	Severity Levels	Service Points
KPI 5	IT Health Check	See paragraph 4 of Part 2 of this Appendix	Annually	Target Performance Level: Zero Vulnerabilities identified without Mitigation Serious KPI Failure: 1-4 vulnerabilities identified without Mitigation KPI Service Threshold: 5 or more identified without Mitigation	0 2 4
KPI 6	Breach of Security	Has the definition set out in Schedule 1 and Part 2 below	Annually	Target Performance Level: Zero Breaches of Security Serious KPI Failure: 1 Breach of Security during the Initial Contract Period, and each subsequent Contract Period thereafter. KPI Service Threshold: More than one Breach of Security during the Initial Contract Period, and each subsequent Contract Period thereafter.	0 10% Annual Contract Value 20% Annual Contract Value

PART 2

DEFINITIONS AND DETERMINATION

1. **AVAILABLE**

1.1 The IT Environment and/or the Services shall be Available when:-

1.1.1 End Users are able to access and utilise all the functions of the Supplier System and/or the Services;

1.1.2 the Supplier System is able to process the Authority Data and to provide any required reports within the timescales set out in the Services Description (as measured on a 24 x 7 basis); and

1.1.3 all Performance Indicators other than Service Availability are above the KPI Service Threshold.

2. SERVICE AVAILABILITY

2.1 Service Availability shall be measured as a percentage of the total time in a Service Period, in accordance with the following formula:-

$$\text{Service Availability \%} = \frac{(MP - SD)\ x100}{MP}$$

where

MP = total number of minutes, excluding Permitted Maintenance, within the relevant Service Period; and

SD = total number of minutes of Service Downtime, excluding Permitted Maintenance, in the relevant Service Period.

2.2 When calculating Service Availability in accordance with this paragraph 2:-

2.2.1 Service Downtime arising due to Permitted Maintenance that is carried out by the Supplier in accordance with Part 1 paragraph 4 shall be subtracted from the total number of hours in the relevant Service Period; and

2.2.2 Service Points shall accrue if:-

(a) any Service Downtime occurs as a result of Emergency Maintenance undertaken by the Supplier; or

3. FIX RATE

3.1 The "**Fix Rate**" of a Service Incident is the percentage of Severity Level 1 Service Incidents reported to the Supplier Resolved on first exchange of messages or within two Working Days (see KP3 and KP4 above respectively) where ‘first exchange of messages’ means the first response of the supplier to once an issue is logged.

3.2 Where "**Resolved**" means in relation to a Service Incident either:-

3.2.1 the root cause of the Service Incident has been removed and the Services are being provided in accordance with the Services Description and Service Levels; or

3.2.2 the Authority has been provided with a workaround in relation to the Service Incident deemed acceptable by the Authority.

3.3 The Supplier shall measure Fix Rates as part of its service management responsibilities and report periodically to the Authority on Fix Rates as part of the Performance Monitoring Report.

4. IT HEALTH CHECKS

4.1 IT Health Checks must be carried out in accordance with Schedule 2.4 paragraph 7.

5. DATA BREACH

5.1 A data breach that does not have any significant impact on or consequences for the Authority and/or Service Recipients will not be considered as a Serious KPI Failure for KPI 6. For clarity, some examples of Data Breach which would indicate a Serious KPI Failure include where a failure in the Supplier system or Supplier support services are responsible for:

a) Unauthorised access to data and/or information that jeopardises the delivery of the Authority's mission to clean up the UK's earliest nuclear sites safely, securely and cost-effectively with care for people and the environment.

b) Unauthorised access to data and/or information that requires a procurement project or contract to be set aside.

c) Unauthorised access to and/or loss of information constituting the Intellectual Property of a third party e.g. information belonging to a bidder or supplier which could result in financial loss to that bidder or supplier and reputational and/or financial impact to the Authority and/or other Service Recipients. In this context, unauthorised access means access by any party other than the Authority and other Service Recipients and the owner of the Intellectual Property. Intellectual Property in this context means copyright, patents, inventions, semiconductor topography, trademarks, designs, knowhow, trade secrets and other confidential information such as pricing, tender submissions and data and information relating to supplier performance.

d) Unauthorised access to and/or loss of any information held in the system which could comprise the security of any Authority sites and/or the sites of other Service Recipients e.g. site drawings or plans.

e) In the unlikely event the Authority requires the system to hold Official-Sensitive Nuclear Information (which would require additional levels of security in the system to be agreed with the Supplier) a breach constitutes the unauthorised access and/or loss of any Official-Sensitive Nuclear Information however small.

f) A GDPR breach where the ICO recommends remedial actions to be made. IT Health Checks must be carried out in accordance with Schedule 2.4 paragraph 7.

SCHEDULE 2.3

STANDARDS

Issue No:	Summary of Change:
V0.1	Version for issue with ITT

I. DEFINITIONS

i. In this Schedule, the definitions set out in Schedule 1 shall apply.

1. GENERAL

1.1 Throughout the Term, the Parties shall monitor and notify each other of any new or emergent standards which could affect the Supplier's provision, or the Authority's or a Service Recipient's receipt, of the Services. Any changes to the Standards, including the adoption of any such new or emergent standard, shall be agreed in accordance with the Change Control Procedure.

1.2 Where a new or emergent standard is to be developed or introduced by the Authority, the Supplier shall be responsible for ensuring that the potential impact on the Supplier's provision, or the Authority's or a Service Recipient's receipt, of the Services is explained to the Authority (in a reasonable timeframe), prior to the implementation of the new or emergent standard.

1.3 Where Standards referenced conflict with each other or with Good Industry Practice, then the later Standard or best practice shall be adopted by the Supplier. Any such alteration to any Standard(s) shall require the prior written agreement of the Authority and shall be implemented within an agreed timescale.

2. TECHNOLOGY AND DIGITAL SERVICES PRACTICE

The Supplier shall (when designing, implementing and delivering any bespoke 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 and agreed with the Contracting Authority.

3. OPEN DATA STANDARDS & STANDARDS HUB

3.1 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.

3.2 Without prejudice to the generality of paragraph 1.2, 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.

3.3 The Supplier shall ensure that all documentation published on behalf of the Authority 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 0 to comply with the UK Government's Open Standards Principles, unless the Authority otherwise agrees in writing.

4. TECHNOLOGY ARCHITECTURE STANDARDS

The Supplier shall produce its standard technical architecture documentation for the Supplier Solution in accordance with Good Industry Practice. If documentation exists that complies with Open Group Architecture Framework 9.2 or its equivalent, then this shall be deemed acceptable.

5. ACCESSIBLE DIGITAL STANDARDS

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

5.1 the World Wide Web Consortium (W3C) Web Accessibility Initiative (WAI) Web Content Accessibility Guidelines (WCAG) 2.1 Conformance Level AA [to be replaced with WCAG 2.2]; or

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

6. SERVICE MANAGEMENT SOFTWARE & STANDARDS

6.1 Subject to paragraphs 1.1.1 to 1.4 (inclusive), the Supplier shall reference relevant industry and HM Government standards and best practice guidelines in the management of the provision of the Services, including the following and/or their equivalents:-

6.1.1 ISO/IEC 20000-1 2018 “Information technology — Service management – Part 1";

6.1.2 ISO/IEC 20000-2 2019 “Information technology — Service management – Part 2";

6.1.3 ISO 10007 "Quality management systems – Guidelines for configuration management";

6.1.4 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 [to be replaced by ISO/IEC AWI 27031];

6.1.5 in accordance with the requirements set out in Schedule 2.4 (Security Requirements):-

(a) ISO/IEC 27001:2013 (or any equivalent as approved by the Authority in writing); and

(b) A commitment to achieve Cyber Essentials Plus before the end of the second year of the contract.

6.2 For the purposes of management of the provision 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.

7. ENVIRONMENTAL STANDARDS

7.1 The Supplier warrants that, at all times during the Term, it and its sub-contractors shall comply with the principles of ISO 14001 (or equivalent) for its environmental management and that of the subcontractors, and shall comply with and maintain compliance throughout the Term. The Supplier shall follow a sound environmental management policy, ensuring that all Goods and the Services are procured, produced, packaged, delivered, and are capable of being used and ultimately disposed of in ways appropriate to such standard.

7.2 The Supplier shall comply with relevant obligations under the Waste Electrical and Electronic Equipment Regulations 2006 in compliance with Directive 2002/96/EC and subsequent replacements (including those in compliance with Directive 2012/19/EU).

7.3 The Supplier shall (when designing, procuring, implementing and delivering the Services) ensure compliance with Article 6 and Appendix III of the Energy Efficiency Directive 2012/27/EU and subsequent replacements.

7.4 The Supplier shall comply with the EU Code of Conduct on Data Centres' Energy Efficiency. The Supplier shall ensure that any data centre used in delivering the Services are registered as a Participant under such Code of Conduct.

7.5 The Supplier shall comply with the Authority and HM Government's objectives to reduce waste and meet the aims of the Greening Government: IT strategy contained in the document "Greening Government: ICT Strategy issue (March 2011)" at https://www.gov.uk/government/publications/greening-government-ict-strategy.

SCHEDULE 2.4

SECURITY MANAGEMENT

Issue No:	Summary of Change:
V0.1	Version for issue with ITT

I. **DEFINITIONS**

i. In this Schedule, the definitions set out in Schedule 1 shall apply.

1. **INTRODUCTION**

1.1 This Schedule sets out:-

1.1.1 the principles which the Supplier shall comply with when performing its obligations under this Agreement in order to ensure the security of the Authority Data, the IT Environment, the Supplier Solution and the Information Management System;

1.1.2 the process which shall apply to the Accreditation of the Core Information Management System in paragraph 1.2;

1.1.3 the Certification Requirements applicable to the Wider Information Management System in paragraph 0;

1.1.4 the Security Tests which the Supplier shall conduct during the Term in paragraph 1.3;

1.1.5 Vulnerability And Penetration Testing (VAPT) is conducted internally on quarterly basis by the Supplier to cover OWASP top-10 vulnerabilities using Burp professional suite. Any vulnerability reported during this testing is remediated on priority basis and this is tracked in ticketing system. Supplier conducts annual external penetration testing which is conducted by an accredited security consultancy. The supplier will share the report upon written request made by Authority.

1.1.6 the requirements to patch vulnerabilities in the Core Information Management System in paragraph 8;

1.1.7 the obligations on the Supplier to prevent the introduction of Malicious Software into the Information Management System and to scan for, contain the spread of, and minimise the impact of Malicious Software which is introduced into the Information Management System in paragraph 0; and

1.1.8 each Party's obligations in the event of an actual or attempted Breach of Security in paragraph 10.

2. PRINCIPLES OF SECURITY

2.1 The Supplier acknowledges that the Authority places great emphasis on the confidentiality, integrity and availability of the Authority Data and, consequently on the security of:-

2.1.1 the IT Environment;

2.1.2 the Supplier Solution; and

2.1.3 the Information Management System.

2.2 Notwithstanding the involvement of the Authority in the Accreditation of the Core Information Management System, the Supplier shall be and shall remain responsible for:-

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

2.2.2 the security of the Supplier Solution; and

2.2.3 the security of the Information Management System.

2.3 The Commercial Systems Governance Board shall, in addition to its responsibilities set out in Schedule 8.1 (*Governance*), monitor and may also provide recommendations to the Supplier on the Accreditation of the Core Information Management System.

2.4 Each Party shall provide access to members of its information assurance personnel to facilitate the Supplier's design, implementation, operation, management and continual improvement of the Risk Management Documentation and the security of the Supplier Solution and Information Management System and otherwise at reasonable times on reasonable notice.

3. INFORMATION MANAGEMENT SYSTEM

3.1 The Information Management System comprises the **"Core Information Management System"** and the **"Wider Information Management System"**.

3.2 The component parts of the Core Information Management System and its boundary with the Wider Information Management System are shown in the diagram in 1.

3.3 Any proposed change to the component parts of and/or boundary of the Core Information Management System shall be notified and processed in accordance with the Change Control Procedure.

4. STATEMENT OF INFORMATION RISK APPETITE AND BASELINE SECURITY REQUIREMENTS

4.1 The Supplier acknowledges that the Authority has provided and the Supplier has received a statement of information risk appetite for the Supplier System and the Services (the "**Statement of Information Risk Appetite**").

4.2 The Authority's Baseline Security Requirements in respect of the Core Information Management System are set out in 1.1.1.

4.3 The Statement of Information Risk Appetite and the Baseline Security Requirements shall inform the Accreditation of the Core Information Management System.

5. ACCREDITATION OF THE CORE INFORMATION MANAGEMENT SYSTEM

5.1 The Core Information Management System shall be subject to Accreditation in accordance with this paragraph 1.2.

5.2 The Accreditation shall be performed by the Authority or by representatives appointed by the Authority.

5.3 Prior to the Operational Services Commencement Date, the Supplier shall prepare and submit to the Authority the risk management documentation for the Core Information Management System, which shall comply with, and be subject to approval by the Authority in accordance with, this paragraph 1.2 (the "**Risk Management Documentation**").

5.4 The Risk Management Documentation shall be structured in accordance with the template as set out in Appendix 4 and include:-

5.4.1 the Accreditation Plan, which shall include:-

(a) the dates on which each subsequent iteration of the Risk Management Documentation will be delivered to the Authority for review and staged approval; and

(b) the date by which the Supplier is required to have received a Risk Management Approval Statement from the Authority together with details of each of the tasks which must be completed by the Supplier, Milestones which must be Achieved and the Authority

Responsibilities which must be completed in order for the Supplier to receive a Risk Management Approval Statement pursuant to paragraph 5.7.1;

5.4.2 a formal risk assessment (SOC Type 2) of the Core Information Management System and a risk treatment plan for the Core Information Management System;

5.4.3 a completed ISO 27001:2013 (or any equivalent as approved by the Authority in writing) Statement of Applicability for the Core Information Management System; the process for managing any security risks from Sub-contractors and third parties authorised by the Authority with access to the Services, processes associated with the delivery of the Services, the Supplier System, Information and data (including the Authority Confidential Information and the Authority Data) and any system under supplier control that could directly or indirectly have an impact on that Information, data and/or the Services;

5.4.4 unless such requirement is waived by the Authority, proposed controls that will be implemented in respect of all aspects of the Services and all processes associated with the delivery of the Services, including the Authority Premises, the Sites, the Supplier System, the Authority System (to the extent that it is under the control of the Supplier) and any IT, Information and data (including the Authority Confidential Information and the Authority Data) to the extent used by the Authority or the Supplier in connection with this Agreement or in connection with any system that could directly or indirectly have an impact on that Information, data and/or the Services;

5.4.5 the Required Changes Register;

5.4.6 evidence that the Supplier and each applicable Sub-contractor is compliant with the Certification Requirements; and

5.4.7 a Personal Data Processing Statement.

5.5 If the Risk Management Documentation submitted to the Authority pursuant to paragraph 1.4 (or paragraph 5.9, as applicable) is approved by the Authority, it shall be adopted by the Supplier immediately and thereafter operated and maintained in accordance with this Schedule. If the Risk Management Documentation is not approved by the Authority, the Supplier shall amend it within ten (10) Working Days of a notice of non--approval from the Authority and re-submit it to the Authority for approval. The Parties shall use all reasonable endeavours to ensure that the approval process takes as little time as possible and in any event no longer than fifteen (15) Working Days (or such other period as the Parties may agree in writing) from the date of its first submission to the Authority. If the Authority does not approve the Risk Management Documentation following its resubmission, the matter shall be resolved in accordance with the Dispute Resolution Procedure. No approval to be given by the Authority pursuant to this paragraph may be unreasonably withheld or delayed. However, any failure to approve the Risk Management Documentation on the grounds that it does not comply with the requirements set out in paragraph 5.4 shall be deemed to be reasonable.

5.6 To facilitate Accreditation of the Core Information Management System, the Supplier shall provide the Authority and its authorised representatives with:-

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

to enable the Authority to establish that the Core Information Management System is compliant with the Risk Management Documentation.

5.7 The Authority shall, by the relevant date set out in the Accreditation Plan, review the identified risks to the Core Information Management System and issue to the Supplier either:-

5.7.1 a Risk Management Approval Statement which will then form part of the Risk Management Documentation, confirming that the Authority is satisfied that the identified risks to the Core Information Management System have been adequately and appropriately addressed and that the residual risks are understood and accepted by the Authority; or

5.7.2 a rejection notice stating that the Authority considers that the residual risks to the Core Information Management System have not been reduced to a level acceptable by the Authority and the reasons why (the "**Risk Management Rejection Notice**").

5.8 If the Authority issues a Risk Management Rejection Notice, the Supplier shall, within twenty (20) Working Days of the date of the Risk Management Rejection Notice:-

5.8.1 address all of the issues raised by the Authority in such notice; and

5.8.2 notify the Authority that the Core Information Management System is ready for an Accreditation Decision.

5.9 If the Authority determines that the Supplier's actions taken pursuant to the Risk Management Rejection Notice have not reduced the residual risks to the Core Information Management System to an acceptable level and issues a further Risk Management Rejection Notice, the failure to receive a Risk Management Approval Statement shall constitute a material Default and the Authority may terminate this Agreement with immediate effect by issuing a Termination Notice to the Supplier in accordance with Clause 29.1 (Termination by the Authority).

5.10 The process set out in paragraph 5.7 and paragraph 5.8 shall be repeated until such time as the Authority issues a Risk Management Approval Statement to the Supplier or terminates this Agreement.

5.11 The Supplier acknowledges that it shall not be permitted to use the Core Information Management System to Process Authority Data prior to receiving a Risk Management Approval Statement.

5.12 The Supplier shall keep the Core Information Management System and Risk Management Documentation under review and shall update the Risk Management Documentation annually in accordance with this paragraph and the Authority shall review the Accreditation Decision annually and following the occurrence of any of the events set out in paragraph 5.13.

5.13 The Supplier shall notify the Authority within two (2) Working Days after becoming aware of:-

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

5.13.2 a new risk or vulnerability is identified to the components or architecture of the Core Information Management System;

5.13.3 a change in the threat profile;

5.13.4 a Sub-contractor failure to comply with the Core Information Management System code of connection;

5.13.5 a significant change to any risk component;

5.13.6 a significant change in the quantity of Personal Data held within the Core Information Management System;

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

5.13.8 an ISO27001 (or any equivalent as approved by the Authority in writing) audit report produced in connection with the Certification Requirements indicates significant concerns,

update the Required Changes Register and provide the updated Required Changes Register to the Authority for review and approval within ten (10) Working Days after the initial notification or such other timescale as may be agreed with the Authority.

5.14 If the Supplier fails to implement a change which is set out in the Required Changes Register by the date agreed with the Authority, such failure shall constitute a material Default and the Supplier shall:-

5.14.1 immediately cease using the Core Information Management System to Process Authority Data until the Default is remedied, unless directed otherwise by the Authority in writing and then it may only continue to Process Authority Data in accordance with the Authority's written directions; and

5.14.2 where such Default is capable of remedy, the Supplier shall remedy such Default within the timescales set by the Authority and, should the Supplier fail to remedy the Default within such timescales, the Authority may terminate this Agreement with immediate effect by issuing a Termination Notice to the Supplier in accordance with Clause 29.1 (*Termination by Authority*).

5.15 The Supplier shall review each Change Request against the Risk Management Documentation to establish whether the documentation would need to be amended should such Change Request be agreed and, where a Change Request would require an amendment to the Risk Management Documentation, the Supplier shall set out any proposed amendments to the documentation in the Impact Assessment associated with such Change Request for consideration and approval by the Authority.

5.16 The Supplier shall be solely responsible for the costs associated with developing and updating the Risk Management Documentation and carrying out any remedial action required by the Authority as part of the Accreditation process.

6. CERTIFICATION REQUIREMENTS

6.1 The Supplier shall ensure, at all times during the Term, that the Supplier and any Sub-contractor with access to Authority Data or who will Process Authority Data are certified as compliant with: -

6.1.1 ISO/IEC 27001:2013 (or any equivalent as approved by the Authority in writing) by a UKAS approved certification body or are included within the scope of an existing certification of compliance with ISO/IEC 27001:2013 (or any equivalent as approved by the Authority in writing); and

6.1.2 a commitment to achieve Cyber Essentials Plus before the end of the second year of the contract; and

6.1.3 shall provide the Authority with a copy of each such certificate of compliance (or suitable evidence of the same as approved by the Authority in writing) before the Supplier or the relevant Sub contractor (as applicable) shall be permitted to use the Core Information Management System to receive, store or Process any Authority Data. Any exceptions to the flow- down of the certification requirements to third party suppliers and sub-contractors must be agreed with the Authority.

The Supplier shall ensure, at all times during the Term, that the Supplier and each Sub-contractor who is responsible for the secure destruction of Authority Data: -

6.1.4 securely destroys Authority Data only on Sites which are included within the scope of an existing certification of compliance with ISO/IEC 27001:2013 (or any equivalent as approved by the Authority in writing); and

6.2 The Supplier shall provide the Authority with evidence of its and its Sub-contractor's compliance with the requirements set out in this paragraph before the Supplier or the relevant Sub-contractor (as applicable) shall be permitted to carry out the secure destruction of the Authority Data.

6.3 The Supplier shall notify the Authority 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 Authority, shall or shall procure that the relevant Sub-contractor shall: -

6.3.1 immediately ceases using the Authority Data; and

6.3.2 procure that the relevant Sub-contractor promptly returns, destroys and/or erases the Authority Data in accordance with Baseline Security Requirements.

7. SECURITY TESTING

7.1 The Supplier shall, at its own cost and expense: -

7.1.1 procure a IT Health Check of the Core Information Management System (an "**IT Health Check**") by an independent agency.:-

(a) within the last 12 months, prior to it submitting the Risk Management Documentation to the Authority for an Accreditation Decision;

7.1.2 once every twelve (12) months during the Term conduct continuous vulnerability scanning and regular annual external assessments and quarterly in-house assessments of the Core Information Management System;

7.1.3 conduct an assessment as soon as reasonably practicable (and in any event, within seventy two (72) hours)) following receipt by the Supplier or any of its Sub-contractors of a critical vulnerability alert from a Supplier of any software or other component of the Core Information Management System to determine whether the vulnerability affects the Core Information Management System; and

7.1.4 conduct such other tests as are required by: -

(a) any Vulnerability Correction Plans;

(b) the ISO27001 (or any equivalent as approved by the Authority in writing) certification requirements;

(c) the Risk Management Documentation; and

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

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

7.2 The Supplier shall provide the Authority up on request the results of such Security Tests (in a form approved by the Authority in advance) as soon as practicable after completion of each Security Test.

7.3 In relation to the IT Health Check, the Supplier shall:-

7.3.1 annually, following receipt of each IT Health Check report, provide the Authority with a copy of the IT Health Check report;

7.3.2 in the event that the IT Health Check report identifies any vulnerabilities without Mitigation, the Supplier shall:-

(a) prepare a remediation plan for approval by the Authority (each a "**Vulnerability Correction Plan**") which sets out in respect of each vulnerability identified in the IT Health Check report: -

(i) how the vulnerability will be remedied or, if a remedy has been proposed by the NCSC approved member of the CHECK Scheme, how that remedy will be implemented;

(ii) the date by which the vulnerability will be remedied;

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

(b) comply with the Vulnerability Correction Plan; and

(c) conduct such further Security Tests on the Core Information Management System as are required by the Vulnerability Correction Plan to confirm that the Vulnerability Correction Plan has been complied with.

7.4 The Security Tests shall be designed and implemented by the Supplier so as to minimise the impact on the delivery of the Services. Subject to the Supplier complying with this paragraph 7.4, if a Security Test causes a Performance Failure in a particular Measurement Period, the Supplier shall be granted relief in respect of such Performance Failure for that Measurement Period.

7.5 Intentionally left blank

7.6 Without prejudice to the provisions of paragraph 7.3.2, where any Security Test carried out pursuant to this paragraph 1.3 reveals any actual or potential Breach of Security or weaknesses (including un-patched vulnerabilities, poor configuration and/or incorrect system management), the Supplier shall promptly notify the Authority of any changes to the Core Information Management System and/or the Risk Management Documentation (and the implementation thereof) which the Supplier proposes to make in order to correct such failure or weakness. The Supplier shall implement such changes to the Core Information Management System and/or the Risk Management Documentation and repeat the relevant Security Tests in accordance with the timetable agreed with the Authority or, otherwise, as soon as reasonably possible.

7.7 If the Authority unreasonably withholds its approval to the implementation of any changes proposed by the Supplier to the Risk Management Documentation in accordance with paragraph **Error! Reference source not found.**, the Supplier shall not be deemed to be in breach of this Agreement to the extent it can be shown that such breach:-

7.7.1 has arisen as a direct result of the Authority unreasonably withholding its approval to the implementation of such proposed changes; and

7.7.2 would have been avoided had the Authority given its approval to the implementation of such proposed changes.

7.8 For the avoidance of doubt, where a change to the Core Information Management System and/or the Risk Management Documentation is required to remedy non-compliance with the Risk Management Documentation, the Baseline Security Requirements and/or any obligation in this Agreement, the Supplier shall effect such change at its own cost and expense.

7.9 If any repeat Security Test carried out pursuant to paragraph 7.6 reveals an actual or potential Breach of Security or weakness exploiting the same root cause failure, such circumstance shall constitute a material Default and the Authority may by terminate this Agreement with immediate effect by issuing a Termination Notice to the Supplier in accordance with Clause 29.1 (Termination by Authority).

7.10 The Supplier shall, by 31 March of each year during the Term, provide to the Authority a letter from its chief executive officer (or equivalent officer) confirming that having made due and careful enquiry:-

7.10.1 the Supplier has in the previous year carried out all tests and has in place all procedures required in relation to security matters under this Agreement; and

7.10.2 the Supplier is confident that its security and risk mitigation procedures with respect to the Services remain effective.

8. VULNERABILITIES AND CORRECTIVE ACTION

8.1 The Authority and the Supplier acknowledge that from time-to-time vulnerabilities in the Information System will be discovered which unless mitigated will present an unacceptable risk to the Authority Data.

8.2 The severity of vulnerabilities for Supplier COTS Software and Third Party COTS Software shall be categorised by the Supplier as 'Critical', 'Important' and 'Other' by aligning these categories to the vulnerability scoring according to the agreed method in the Risk Management Documentation and using the appropriate vulnerability scoring systems including: -

8.2.1 the 'National Vulnerability Database' 'Vulnerability Severity Ratings': 'High', 'Medium' and 'Low' respectively (these in turn are aligned to CVSS scores as set out by NIST at http://nvd.nist.gov/cvss.cfm); and

8.2.2 Microsoft's 'Security Bulletin Severity Rating System' ratings 'Critical', 'Important', and the two remaining levels ('Moderate' and 'Low') respectively.

8.3 Subject to paragraph 8.4, the Supplier shall procure the application of security patches to vulnerabilities in the Core Information Management System within: -

8.3.1 seven (7) days after the public release of patches for those vulnerabilities categorised as 'Critical';

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

8.3.3 sixty (60) days after the public release of patches for those vulnerabilities categorised as 'Other'.

8.4 The timescales for applying patches to vulnerabilities in the Core Information Management System set out in paragraph 8.3 shall be extended where: -

8.4.1 the Supplier can demonstrate that a vulnerability in the Core Information Management System is not exploitable within the context of the Services (eg 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 8.3 if the vulnerability becomes exploitable within the context of the Services;

8.4.2 the application of a 'Critical' or 'Important' security patch adversely affects the Supplier's ability to deliver the Services in which case, the Supplier shall provide the Authority with all necessary evidence of the adverse effects on Service delivery and, provided that the Authority agrees (acting reasonably) with the Supplier, then 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 Authority; or

8.4.3 the Authority agrees a different maximum period after a case--by--case consultation with the Supplier under the processes defined in the Risk Management Documentation.

8.5 The Risk Management Documentation shall include provisions for major version upgrades of all Supplier COTS Software and Third Party COTS Software to be kept up to date such that all Supplier COTS Software and Third Party COTS Software are always in mainstream support throughout the Term unless otherwise agreed by the Authority in writing.

8.6 The Supplier shall: -

8.6.1 implement a mechanism for receiving, analysing and acting upon threat information supplied by NCSC, or any other competent Central Government Body;

8.6.2 promptly notify NCSC of any actual or sustained attempted Breach of Security;

8.6.3 ensure that the Core Information Management System is monitored to facilitate the detection of anomalous behaviour that would be indicative of system compromise;

8.6.4 ensure it is knowledgeable about the latest trends in threat, vulnerability and exploitation that are relevant to the Core Information Management System by actively monitoring the threat landscape during the Term;

8.6.5 pro-actively scan the Core Information Management System for vulnerable components and address discovered vulnerabilities through the processes described in the Risk Management Documentation;

8.6.6 from the date specified in the Accreditation Plan and within five (5) Working Days of the end of each subsequent month during the Term, provide the Authority 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 8.3 for applying patches to vulnerabilities in the Core Information Management System;

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

8.6.8 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 Core Information Management System); and

8.6.9 inform the Authority when it becomes aware of any new threat, vulnerability or exploitation technique that has the potential to affect the security of the Core Information Management System and provide initial indications of possible mitigations.

8.7 If the Supplier is unlikely to be able to mitigate the vulnerability within the timescales under paragraph 0, the Supplier shall immediately notify the Authority.

8.8 If the Supplier fails to patch vulnerabilities in the Core Information Management System in accordance with paragraph 8.3, such failure shall constitute a material Default and the Authority may by terminate this Agreement with immediate effect by issuing a Termination Notice to the Supplier in accordance with Clause 29.1 (Termination by Authority).

9. MALICIOUS SOFTWARE

9.1 The Supplier shall install and maintain anti--Malicious Software or procure that latest versions of anti-virus definitions and anti--Malicious Software is installed and maintained on any part of the Information Management System, which may Process Authority Data and ensure that such anti--Malicious Software is configured to perform automatic software and definition updates as well as regular scans of the Information Management System to check for, prevent the introduction of Malicious Software or where Malicious Software has been introduced into the Information Management System, to identify, contain the spread of, and minimise the impact of Malicious Software.

9.2 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 Authority Data, assist each other to mitigate any Losses and to restore the provision of the Services to their desired operating efficiency.

9.3 Any cost arising out of the actions of the Parties taken in compliance with the provisions of paragraph 9.2 shall be borne by the Parties as follows:-

9.3.1 by the Supplier where the Malicious Software originates from the Supplier Software, the Third Party Software supplied by the Supplier (except where the Authority has waived the obligation set out in Clause 19.13 (*Malicious Software*)) or the Authority Data (whilst the Authority 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 Authority when provided to the Supplier; and

9.3.2 otherwise by the Authority.

10. BREACH OF SECURITY

10.1 If either Party becomes aware of a Breach of Security or an attempted Breach of Security it shall notify the other in accordance with the security incident management process as set out in the Risk Management Documentation.

10.2 The security incident management process set out in the Risk Management Documentation shall, as a minimum, require the Supplier upon becoming aware of a Breach of Security or an attempted Breach of Security to:-

10.2.1 immediately take all reasonable steps (which shall include any action or changes reasonably required by the Authority which shall be completed within such timescales as the Authority 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 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 and, provided that reasonable testing has been undertaken by the Supplier, if the mitigation adversely affects the Supplier's ability to deliver the Services so as to meet any Performance Indicator, the Supplier shall be granted relief against the failure to meet such affected Performance Indicator for such period as the Authority, acting reasonably, may specify by written notice to the Supplier; and

(d) prevent a further Breach of Security or attempted Breach of Security in the future exploiting the same root cause failure;

10.2.2 as soon as reasonably practicable and, in any event, verbally within forty eight (48) hours and in written form within seventy two (72) hours, following the Breach of Security or attempted Breach of Security, provide to the Authority full details of the Breach of Security or attempted Breach of Security, including a root cause analysis where required by the Authority.

10.3 In the event that any action is taken in response to a Breach of Security or attempted Breach of Security which occurred as a result of non-compliance of the Information System and/or the Risk Management Documentation with the Baseline Security Requirements and/or this Agreement, then such action and any required change to the Information System and/or Risk Management Documentation shall be completed by the Supplier at no cost to the Authority.

10.4 If the Supplier fails to comply with its obligations set out in this paragraph 10, such failure shall constitute a material Default, which if not remedied to the satisfaction of the Authority, shall permit the Authority to terminate this Agreement with immediate effect by issuing a Termination Notice to the Supplier in accordance with Clause 29.1 (*Termination by the Authority*).

11. DATA PROCESSING, STORAGE, MANAGEMENT AND DESTRUCTION

11.1 In addition to the obligations on the Supplier set out Clause 22 (*Protection of Personal Data*) in respect of Processing Personal Data and compliance with the Data Protection Legislation, the Supplier shall:-

11.1.1 Process Authority Data only at the Sites and such Sites must not be located outside of the United Kingdom except where the Authority has given its consent to a transfer of the Authority Data to outside of the United Kingdom in accordance with Clause 22 (*Protection of Personal Data*);

11.1.2 on demand, provide the Authority with all Authority Data in an agreed open format;

11.1.3 have documented processes to guarantee availability of Authority Data in the event of the Supplier ceasing to trade;

11.1.4 securely erase any or all Authority Data held by the Supplier when requested to do so by the Authority; and

11.1.5 securely destroy all media that has held Authority 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 directed by the Authority.

APPENDIX 2

BASELINE SECURITY REQUIREMENTS

12. SECURITY CLASSIFICATION OF INFORMATION

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

13. END USER DEVICES

13.1 The Supplier shall ensure that any Authority 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 Authority except where the Authority has given its prior written consent to an alternative arrangement.

13.2 The Supplier shall ensure that any device which is used to Process Authority 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/guidance/end-user-device-security.

14. NETWORKING

The Supplier shall ensure that any Authority 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 in accordance with Good Industry Practice.

15. PERSONNEL SECURITY

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

15.2 The Authority 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 Authority to determine which roles require additional vetting and a specific national security vetting clearance (e.g. a Counter Terrorist Check; a Security Check). Roles which may require additional vetting and a specific national security vetting clearance include system administrators whose role would provide those individuals with privileged access to IT systems which Process Authority Data or data which is classified OFFICIAL--SENSITIVE.

15.3 The Supplier shall not permit Supplier Personnel who fail the security checks required by paragraphs 3.1 and 3.1 to be involved in the management and/or provision of the Services except where the Authority has expressly agreed in writing to the involvement of the named individual in the management and/or provision of the Services.

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

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

16. IDENTITY, AUTHENTICATION AND ACCESS CONTROL

16.1 The Supplier shall operate an access control regime to ensure:-

16.1.1 all users and administrators of the Supplier System are uniquely identified and authenticated (using multiple-factor authentication utilizing the Authority's Single Sign On processes in accordance with Good Industry Practice) when accessing or administering the Services; and

16.1.2 all persons who access the Sites are identified and authenticated before they are allowed access to the Sites.

16.2 The Supplier shall apply the 'principle of least privilege' when allowing persons access to the Supplier System and Sites so that such persons are allowed access only to those parts of the Sites and the Supplier System they require.

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

17. AUDIT AND PROTECTIVE MONITORING

17.1 The Supplier shall collect audit records which relate to security events in the 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 Information Management System, to enable the identification of (without limitation) changing access trends, any unusual patterns of usage and/or accounts accessing higher than average amounts of Authority Data.

17.2 The Supplier and the Authority shall work together to establish any additional audit and monitoring requirements for the Information Management System.

17.3 The retention periods for audit records and event logs must be agreed with the Authority and documented in the Risk Management Documentation.

18. SECURE ARCHITECTURE

18.1 The Supplier shall ensure that the Core Information Management System meets the requirements of :-

18.1.1 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;

18.1.2 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

18.1.3 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 Authority Data and/or the Authority 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 Authority to securely manage the Authority'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 Authority with the audit records it needs to monitor access to the Service and the Authority Data held by the Supplier and/or its Sub-contractors;

(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.

19. **OFFICIAL--SENSITIVE NUCLEAR INFORMATION**

19.1 Within the UK, regulation of the Civil Nuclear Industry's Supply Chain, and specifically holders of Sensitive Nuclear Information (SNI) outside of nuclear facilities, falls under Regulation 22 of the Nuclear Industries Security Regulations (NISR) 2003. Should the unlikely need arise for the Supplier Solution to hold Official--Sensitive Nuclear Information, the Supplier shall maintain such security standards, procedures and arrangements as are necessary for the purpose of minimising the risk of loss, theft or unauthorised disclosure of, or unauthorised access to, any SNI.

19.2 System administrators and other Supplier Personnel whose role would provide those individuals with privileged access to IT systems which Process Authority Data or data classified at OFFICIAL--SENSITIVE--SNI will require national security vetting clearance at Security Check level. Where the Authority requires system administrators or other Supplier Personnel to hold Security Check vetting clearance, the Authority will sponsor the Supplier through the vetting process and accept the costs in accordance with Schedule 7.1 (*Charges and Invoicing*).

19.3 The Supplier shall work with the Authority to certify its system to SNI levels prior to any OFFICIAL--SENSITIVE--SNI information being held in the system. The Authority will accept all reasonable costs incurred by the Supplier in certifying its system to SNI levels in accordance with Schedule 7.1 (*Charges and Invoicing*).

1. There was concern around the difference in entering into a contract and the amendment to a contract. This needs to be separated or made clear that amending an existing contract must be compliant under PCR and within the allowable value of the existing contract. For example allowable extensions versus increasing contract value above 50% etc
2. Value limit VAT or No VAT
3. Signing of contracts – Are we agreeing that this is also signature value or is there an argument that as long as Emma or Steve has approved, then anyone within commercial can sign? In addition, are we allowing commercial colleagues to sign their own contracts (marking their own homework) or should this be passed to a colleague to sign with the appropriate level of authority.
4. Are we going to allow the delegated authority within own category in the absence of a LM for example.
5. Frameworks – Are we allowing the approval of frameworks under delegated authority where there is no value but ultimately there could be significant spend via that framework.
6. We discussed that the delegated authority needs to be managed sensitively, we understand that the value will be based on relative experience and the value that the individual maybe comfortable with. However we need to be open and transparent so this needs to be a considered approach.

7. Fraud policies need to be referenced in some way and some guidance on who we pass to for signing not the same friend for example.
8. Sage – Thoughts on making changes within the Sage system to reflect the authority levels.

APPENDIX 3 [Redacted for Publication]

APPENDIX 4

RISK MANAGEMENT DOCUMENTATION TEMPLATE

Author:-

Owner:-

Date:-

Version:-

20. **EXECUTIVE SUMMARY**

20.1 Resilinc a supply chain risk management platform and multi-enterprise network connecting suppliers efficiently on a single platform to allow them to quickly provide visibility to their sites, parts and suppliers to many customers without duplicating efforts. Resilinc's patented risk intelligence and analytics solution greatly simplifies the supply risk management journey for customers.

20.2 Resilinc will allow the NDA to manage supply chain risk more effectively with its multi-tier supply chain mapping, risk quantification and continuous disruption monitoring solutions; building an information highway that forms the backbone for resilient supply chains.

Change History

Version Number	Date of Change	Change made by	Nature and reason for change

References, Links and Dependencies

This document is dependent on the supporting information and assurance provided by the following documents.

ID	Document Title	Reference	Date
1.			

2.			
3.			

21. SYSTEM DESCRIPTION

21.1 Background

21.1.1 In response to the tender for the NDA Commercial Systems Procurement Lot D – Supply Chain Mapping and Risk Management System, Resilinc provides a single cohesive system to manage end-to-end supply chain risk and resiliency.

21.1.2 Resilinc a supply chain risk management platform and multi-enterprise network connecting suppliers efficiently on a single platform to allow them to quickly provide visibility to their sites, parts and suppliers to many customers without duplicating efforts. Resilinc's patented risk intelligence and analytics solution greatly simplifies the supply risk management journey for customers.

21.2 Organisational Ownership/Structure

21.2.1 Resilinc maintains ownership of the SaaS platform.

21.2.2 The Resilinc top management is committed to information security and set the direction for scope, performance, and improvement of the Information Security Management System. Top Management is part of Management Review Meetings which are held bi-annually. These meetings ensure to review and evaluate the performance of information security policy. The regular feedback from interested parties is discussed in these meetings to understand if any change in the processes should be implemented. We ensure integrity of information by performing scheduled third-party audits for ISO 27001 and SOC2 type 2 assessment so that the internal controls are verified by a third party. The supplier will provide Authority with copies of ISO 27001 and SOC2 Type 2 certificates after every annual renewal over the initial contract term.

21.3 Information assets and flows

See typical information flow detailed below:

Client request comes from Internet, via firewall to the Load Balancer. Only HTTPS requests are allowed, and other requests are filtered out at the firewall.

The Load Balancer forwards the request to one of the public slave nodes in DC/OS cluster in round robin fashion.

According to the service requested, built-in proxy in the public slave node forwards the request to private slave node where the requested microservice is currently running. In case, if multiple instances of such service are running, the public slave acts like a load balancer as well.

The service authenticates the requester by consulting with the identity server.

The client session, if new one is getting created, is installed in the Redis server's keystore. Authentication token is returned to the client in the response. Every subsequent request must contain this authentication token.

Client, once authenticated, can request for data. The request containing valid authentication token is sent to the firewall from client side.

Firewall, if it is a HTTPS request, sends it to the Load Balancer. The Load Balancer sends the request to one of the public slave nodes on DC/OS in round robin fashion.

The request is forwarded to one of the private slave nodes of DC/OS where the requested service is running.

The service consults with the Redis server to validate the client's session. Any request, not having valid session information, is rejected by the service.

For the authenticated request, the service talks to the database via PGBouncer which is a connection pooling manager for the Postgres instance. The CRUD operation is performed on the database and the requested information is returned by the service to the client.

Read replica of the primary Postgres instance is kept in sync in real time by Barman running in the database layer. WAL shipping is done from Primary database to Barman server for performing recovery

21.4 System Architecture

Resilinc's solution is a multi-tenant Software as a Service (SaaS) solution hosted on the IBM Cloud. Its multi-tenant architecture logically segments the database between tenants. Each tenant is only allowed access to the data in its section. To achieve strict tenant separation, Resilinc has implemented a Data Access Layer that controls access to the database. Regardless of the type of access (Create, Read, Update, Delete), all transactions go through the Data Access Layer.
See solution architecture diagram below for further detail:

[Redacted for Publication]

21.5 Users

Resilinc admin: Initially Admin user (Resilinc) will work along with Company Admin user (Customer) for onboarding additional users & managing roles/access of new users. Also, work with Admin user to configure org & set-up org as per requirement based on Category, Role, region etc.
Company Admin: Post initial training from Resilinc Customer Success Manager (CSM), Company Admin (Customer) user is responsible to onboard and activate/deactivate customer users. Managing roles and responsibilities of customer application users will be responsibility of Admin user. Apart from this, Company Admin user will also set-up companywide global settings for EventWatch notifications and configure risk thresholds.
Admin user is also responsible for loading of customer data in the desired format with Customer Success Manager available for support.
Application Users: User will be responsible to perform one or more of the following tasks,

- Set-up personal settings to configure of EventWatch notification preferences
- Keep track of survey progress. In case of escalations of survey take required action to extend or terminate survey

Access of all application users can be controlled by module, category, NDA subsidiary, department etc. The application access is monitored and reviewed on a quarterly basis. This exercise includes to review privileged / Admin access. The ability to create or modify users and user access privileges is limited.

21.6 **Locations**

21.7 Resilinc solution is a cloud-based Software As A Service (SaaS), deployed on IBM Cloud. All the data centres used are located in the USA. The locations are Richardson-Texas, San Jose-California and Ashburn-Virginia. **Test and Development Systems**

Resilinc has test and development systems in our Pune India offices. These systems do not contain any live customer data.

21.8 **Key roles and responsibilities**

Each of the following business units lead security and incident management within Resilinc:
- Information Security Office: Determine the nature and scope of the any security incidents
- Information Technology – Operations & Infrastructure: Act as a central point of contact for reporting any security incidents
- Business Applications: Conduct ongoing monitoring of business applications and services
- Internal Auditing: Reviews systems to ensure compliance with information security policy and controls

22. **RISK ASSESSMENT**

22.1 **Accreditation/Assurance Scope**

Resilinc's data security and maintenance is certified on ISO 27001:2013, ISO 9001:2015 and SOC 2 Type II. This ensures that Resilinc have the necessary framework in place so that practices are in line with industry standards without compromise.
Resilinc solution is hosted on IBM Cloud. All the infrastructure aspects in the data centres are managed by IBM Cloud.

- IBM platform services, used to manage the infrastructure, have SLA of 99.99% availability.
- All cloud data centres maintain multiple power feeds, fibre links, dedicated generators, and battery backup to avoid a single-point-of-failure (SPOF)
- Cloud network is designed in such a way that there is never a single point of failure. Diverse and redundant connectivity exists at every point of the network, by using diverse telecommunication providers for the same service connectivity.
- Their Disaster Recovery and Business Continuity Plan practices are in line with various standards that they comply with. These are the relevant compliance programs IBM adhere to.
  - ISO 9001
  - ISO 27001
  - SOC 1 / 2 / 3
  - HIPAA, PCI

22.2 **Risk appetite**

The Authority's statement of risk appetite is embedded below.

22.3 **Business impact assessment**

22.4 Resilinc's software is hosted on IBM Cloud. As a result, Resilinc maintains computer servers, web servers, or databases. In case of any security breach such as loss or corruption of data, Resilinc will follow established procedure to stop the breach and will notify any affected Customers within 24 hours of Resilinc determining the extent of the breach.

22.5 **Risk assessment**

Risk ID	Inherent risk	Inherent risk level	Vulnerability	Controls	Residual risk level
R1	Internet attackers could hack the system.	High	The service systems are exposed to the internet via the web portal.	C1: Internet-facing firewalls C3: System hardening C4: Protective monitoring C5: Application access control C16: Anti-virus for incoming files	Medium
R2	Remote attackers could intercept or disrupt information crossing the internet.	Medium	File sharing with organisations across the internet.	C9: Data encryption	Low

R3	Internal users could maliciously or accidentally alter data.	Medium-High	Customer data can be altered as part of the normal business function.	All system and user rights audited Staff awareness training	Low

22.6 **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.>

This information will be added within the progression of the Security Assessment completed with the Authority. This process is currently ongoing and will be completed as soon as possible.

[Redacted For Publication]

23. **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 (or any equivalent as approved by the Authority in writing) certification should be included. This section should include at least:-

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

Resilinc management is committed to information security and set the direction for scope, performance, and improvement of the Information Security Management System. Top Management is part of Management Review Meetings which are held bi-annually. These meetings ensure to review and evaluate the performance of information security policy. The regular feedback from interested parties is discussed in these meetings to understand if any change in the processes should be implemented. We ensure integrity of information by performing scheduled third-party audits for ISO 27001 and SOC2 type 2 assessment so that the internal controls are verified by a third party.

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

As Resilinc is hosted on IBM cloud, all security and infrastructure patching is managed by IBM.

23.3 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;

The application performs the following logging:
1. System Events: Operational actions performed by OS components, including shutting down the system or starting a service.
2. Audit Logs of relevant security event information:
3.Authentication & Login attempts
4.Account changes (account creation/deletion, account privilege assignment)
5.Use of privileges

Resilinc has implemented a comprehensive audit system that logs changes to every column of every row in every table automatically. No users have control over this functionality i.e. no user can disable it. Auditing is automatic and cannot be turned off. It is a part of the database.

Resilinc has a well-managed monitoring system and procedure in place. We use standard monitoring tools like Nagios, Prometheus, etc. Phone/SMS/email-based alerts are generated for the infrastructure team from these tools. We also use an external synthetic monitoring tool to monitor the uptime of our application.

23.4 configuration and change management;

A deployable product increment, a patch, or an infrastructure upgrade is planned by the Engineering team on the request of Operations or Product Management Team. The Change initiates after the final approval of the Product Management Team

23.5 incident management;

Resilinc has an Incident Response Team that is responsible for providing a timely and effective response to any actual or suspected Security Incident. The Team is authorized to take appropriate steps deemed necessary to investigate, mitigate, and resolve Security Incidents. The Team is responsible for reporting its findings to management and the appropriate authorities as necessary

23.6 vulnerability management;

Resilinc conducts a quarterly internal VAPT covering OWASP top-10 vulnerabilities. As well as annual external penetration testing by engaging an accredited security consultancy.

23.7 user access management; and

IBM Cloud is an Infrastructure Cloud Provider (IaaS) and the firewall secures access to IBM Cloud. Network on which Resilinc Software is deployed. The Data Isolation is governed by Multi-Tenancy. For security reasons, suppliers cannot login to Customer’s Tenant and vice-versa. In general, any user cannot login with another tenant except his own.

For user access within the Resilinc tool, user provisioning/deprovisioning, roles and access rights can be managed centrally by appointed admin users.

23.8 data sanitisation and disposal.>

All users are responsible for the secure creation, storage, amendment, copying, and deletion/destruction of information.
Data Disposal/Destruction
Electronic and physical data must be destroyed following the Data Deletion Procedure.
Appropriate authorizations are taken before data/document disposal.
Upon Customer separation, Resilinc contacts the customer to confirm the method of data transition/disposal. Post customer approval/as per customer agreement the data is either archived and placed on secure FTP for Customer retrieval or deleted.

24. SECURITY OPERATING PROCEDURES (SYOPS)

Resilinc's software is hosted on IBM Cloud. As a result, Resilinc maintains computer servers, web servers, or databases. In case of any security breach, Resilinc will follow the procedure as per Incident Management and will notify its Customers not less than 72 hours

25. INCIDENT MANAGEMENT PROCESS

Resilinc has an Incident Response Team that is responsible for providing a timely and effective response to any actual or suspected Security Incident. The Team is authorized to take appropriate steps deemed necessary to investigate, mitigate, and resolve Security Incidents. The Team is responsible for reporting its findings to management and the appropriate authorities as necessary.
A Management Representative will coordinate the activities of the Team. Each of the following business units will have a team member:

- Information Security Office
- Information Technology - Operations & Infrastructure
- Law Department (Not part of the internal group, however will be involved as per the requirement)
- Business Applications
- Internal Auditing

26. SECURITY REQUIREMENTS FOR USER ORGANISATIONS

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

27. 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.	Authority name	11/11/2018	Jul-2019	Open

28. **PERSONAL DATA PROCESSING STATEMENT**

Personal data such as name, contact number, official email id will be processed.

NDA's data including personal data always resides in the production environment in cloud infrastructure (IBM cloud). It is saved in encrypted form. Customer data is not stored on PCs, laptops, or portable media. IBM data centers are in the United States. IBM Cloud does not have access to the Customer data. Resilinc has a development center in Pune, India.

29. **APPENDIX A. ISO27001 (OR ANY EQUIVALENT AS APPROVED BY THE AUTHORITY IN WRITING) AND/OR CYBER ESSENTIAL PLUS CERTIFICATES**

30. **APPENDIX B. CLOUD SECURITY PRINCIPLES ASSESSMENT**

31. Resilinc solution is hosted on IBM Cloud. All cloud security principles are observed by IBM.

32. **APPENDIX D. LATEST ITHC REPORT AND VULNERABILITY CORRECTION PLAN**

SCHEDULE 2.5

INSURANCE REQUIREMENTS

Issue No:	Summary of Change:
V0.1	Version for issue with ITT

INSURANCE REQUIREMENTS

33. **OBLIGATION TO MAINTAIN INSURANCES**

33.1 Without prejudice to its obligations to the Authority 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 1.2 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.

33.2 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 operating the same or substantially similar business in respect of risks insured in the international insurance market from time to time.

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

33.3.1 of good financial standing;

33.3.2 appropriately regulated;

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

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

33.4 The Supplier shall ensure that the public and products liability policy shall contain an indemnity to principals clause under which the Authority shall be indemnified in respect of claims made against the Authority 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.

34. GENERAL OBLIGATIONS

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

34.1 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;

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

34.3 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.

35. FAILURE TO INSURE

35.1 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 cancel, rescind or suspend any of the Insurances or cover, or to treat any of the Insurances, cover or claim as avoided in whole or in part refuse to pay any claim under any of the Insurances.

35.2 Where the Supplier has failed to purchase any of the Insurances or maintain any of the Insurances in full force and effect, the Authority may elect (but shall not be obliged) following written notice to the Supplier to purchase the relevant Insurances, and the Authority shall be entitled to recover the reasonable premium and other reasonable costs incurred in connection therewith as a debt due from the Supplier.

36. EVIDENCE OF INSURANCES

36.1 The Supplier shall upon the Effective Date provide evidence, in a form satisfactory to the Authority, that the Insurances are in force and effect and meet in full the requirements of this Schedule. Receipt of such evidence by the Authority shall not in itself constitute acceptance by the Authority or relieve the Supplier of any of its liabilities and obligations under this Agreement.

36.2 If the Insured is required to provide Insurance beyond the end of the Term by this Agreement, then the Supplier shall continue to provide such evidence as set out in and in accordance with paragraph 36.1 for so long as this requirement continues.

36.3 The Supplier shall also provide any further information reasonably requested by the Authority in relation to the Insurances at any time during the Term on reasonable notice.

37. CANCELLATION

37.1 Subject to paragraph 0, the Supplier shall notify the Authority in writing at least thirty (30) Working Days prior to the cancellation, suspension, termination or non-renewal of any of the Insurances.

37.2 Without prejudice to the Supplier's obligations under paragraph 1.1.1, paragraph 1.4 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.

38. INSURANCE CLAIMS, PREMIUMS AND DEDUCTIBLES

38.1 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 Authority receives a claim relating to or arising out of the Services and/or this Agreement, the Supplier shall co-operate with the Authority and assist it in dealing with such claims at its own expense including without limitation providing information and documentation in a timely manner.

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

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

38.4 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 Authority any sum paid by way of excess or deductible under the Insurances whether under the terms of this Agreement or otherwise.

39. LIMIT OF LIABILITY

39.1 Neither failure to comply, nor full compliance, with the insurance provisions of the Agreement shall limit or relieve the Supplier of its other liabilities and obligations under this Agreement.

APPENDIX 5

REQUIRED INSURANCES

PART 1

INSURANCE CLAIM NOTIFICATION

Except where the Authority is the claimant party, the Supplier shall give the Authority notice within twenty (20) Working Days after any insurance claim in excess of one hundred thousand pounds sterling £100,000 relating to or arising out of the provision of the Services or this Agreement on any of the Insurances or which, but for the application of the applicable policy excess, would be made on any of the Insurances and (if required by the Authority) full details of the incident giving rise to the claim.

PART 2

THIRD PARTY PUBLIC AND PRODUCTS LIABILITY INSURANCE

40. **INSURED**

The Supplier.

41. **INTEREST**

To indemnify the Insured in respect of all sums which the Insured shall become legally liable to pay as damages, including claimant's costs and expenses, in respect of accidental:-

41.1 death or bodily injury to or sickness, illness or disease contracted by any person; and

41.2 loss of or damage to physical property;

happening during the period of insurance (as specified in paragraph 0) and arising out of or in connection with the provision of the Services and in connection with this Agreement.

42. **LIMIT OF INDEMNITY**

42.1 Not less than Two Hundred and Fifty Thousand Pounds (£250,000) in respect of any one occurrence, , but One Million Pounds (£1 million) in the aggregate per annum in respect of products liability.

43. **TERRITORIAL LIMITS**

43.1 The Supplier shall meet its insurance obligations under United Kingdom Law in full as set out in Appendix 5.

44. **PERIOD OF INSURANCE**

A minimum insurance period of 3 years following the expiration or Ending of this Agreement unless agreed otherwise by the Authority in writing.

45. **COVER FEATURES AND EXTENSIONS**

45.1 Indemnity to principals clause under which the Authority shall be indemnified in respect of claims made against the Authority 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.

46. **PRINCIPAL EXCLUSIONS**

46.1 War and related perils.

46.2 Nuclear and radioactive risks.

46.3 Liability for death, illness, disease or bodily injury sustained by employees of the Insured arising out of the course of their employment.

46.4 Liability arising out of the use of mechanically propelled vehicles whilst required to be compulsorily insured by applicable Law in respect of such vehicles.

46.5 Liability in respect of predetermined penalties or liquidated damages imposed under any contract entered into by the Insured.

46.6 Liability arising out of technical or professional advice other than in respect of death or bodily injury to persons or damage to third party property.

46.7 Liability arising from the ownership, possession or use of any aircraft or marine vessel.

46.8 Liability arising from seepage and pollution unless caused by a sudden, unintended and unexpected occurrence.

47. **MAXIMUM DEDUCTIBLE THRESHOLD**

Not to exceed £250 for each and every third party property damage claim (personal injury claims to be paid in full).

PART 3

UNITED KINGDOM COMPULSORY INSURANCES

The Supplier shall meet its insurance obligations under applicable Law in full, including, United Kingdom employers' liability insurance and motor third party liability insurance.

PART 4

ADDITIONAL INSURANCES

The Supplier shall meet as a minimum the insurance obligations as set out below:-

Employer's (Compulsory) Liability Insurance	employer's liability insurance in accordance with any legal requirement for the time being in force in relation to any one claim or series of claims"
Public Liability Insurance	£1 million in respect of each claim, and in the annual aggregate
Professional Indemnity Insurance	£1 million in the annual aggregate
Product Liability Insurance	£1 million in the annual aggregate
Cyber and Data Insurance	£1 million in the annual aggregate

SCHEDULE 3

AUTHORITY RESPONSIBILITIES

Issue No:	Summary of Change:
V0.1	Version for issue with ITT

1. **INTRODUCTION**

1.1 The responsibilities of the Authority set out in this Schedule shall constitute the Authority Responsibilities under this Agreement. Any obligations of the Authority in Schedule 2.1 (*Services Description*) and Schedule 4.1 (*Supplier Solution*) shall not be Authority Responsibilities and the Authority shall have no obligation to perform any such obligations unless they are specifically stated to be "Authority Responsibilities" and cross referenced in the table in paragraph 1.2.

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

1.3 Any capitalised terms used in this Schedule that are not defined in Schedule 1 (*Definitions*) shall have the meanings as defined in Schedule 2.1 (*Service Description*).

2. **GENERAL OBLIGATIONS**

The Authority shall:-

2.1 perform those obligations of the Authority 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*));

2.2 use its reasonable endeavours to provide the Supplier with access to appropriate members of the Authority'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;

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

2.4 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 Authority and is authorised for release by the Authority; and

2.5 procure for the Supplier such agreed access and use of the Authority 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 Authority's normal working hours on each Working Day or as otherwise agreed by the Authority (such agreement not to be unreasonably withheld or delayed).

3. SPECIFIC OBLIGATIONS

3.1 The Authority shall, in relation to this Agreement perform the Authority's obligations identified as such in this Agreement the details of which are set out in Appendix 1 where the following definitions shall apply:-

3.1.1 "Responsible" shall have the meaning to have the job or duty of completing a task to enable the Supplier to deliver its obligations under this Agreement, for example reviewing or signing off documents;

3.1.2 "Accountable" shall have the meaning to be responsible for making sure decisions and actions are undertaken by the Authority and/or Service Recipients and that outputs meet the Authority's requirements to enable the Supplier to deliver its obligations under this Agreement; and

3.1.3 "Support Role" shall have the meaning to provide assistance to the Supplier to enable the Supplier to perform its obligations under the contract, for example to identify gaps between the Supplier Solution and Authority requirements.

4. ADDITIONAL OBLIGATIONS

4.1 The Authority Responsibilities as set out in Appendix 1 and Appendix 2 of Schedule 6.1 *(Implementation Plan)* shall also apply.

APPENDIX 1

AUTHORITY OBLIGATIONS

Not used

SCHEDULE 4.1

SUPPLIER SOLUTION

Issue No:	**Summary of Change:**
V0.1	Version for issue with ITT

[**Bidder Note: All relevant parts of the Supplier's response to this Schedule and any other Supplier-provided documents shall be included as additional appendices to this Schedule. The Supplier's response must include material relating to the headings of the sections in Volume 3, and the Supplier may add further material relevant to the Solution and the Authority's requirements documented in the Agreement:**

- Overview of the Supplier Solution;
- Security, user management and experience;
- Master data management;
- Supply Chain Mapping and Supplier Engagement
- Risk Analysis, Management, Mitigation and Event Monitoring

- Reporting and interfaces;
- Training and support;
- Mobilisation and configuration; and
- Any additional sections as appropriate.

1. **DEFINITIONS**

1.1 In this Schedule, the definitions set out in Schedule 1 shall apply.

2. **DATA PROCESSING PARTICULARS**

2.1 **The data processing particulars referred to in Clause 22 (Protection of Personal Data) are included in Appendix 1.**

3. **SUPPLIER SOLUTION**

3.1 **The Supplier Solution comprises the Supplier Solution Overview in Appendix 2 and the Supplier's response to the Invitation To Tender in Appendix 3.**

APPENDIX 1

DATA PROCESSING PARTICULARS

These are the data processing particulars referred to in Clause 22 (Protection of Personal Data).

[Bidder Note: This table will be completed using the information supplied as part of the Invitation to Tender Response.]

Data Processing Particulars	Details of Data Processing
The subject matter and duration of the Processing	Personal data as described in this table will be uploaded to the Supplier Solution to enable the Supplier to provide the Services.
The nature and purpose of the Processing	Personal data is required to enable the Supplier to provide supply chain risk management and mapping services by way of the Supplier Solution, for example, contact details for key contacts at the Authority's suppliers will be processed on the Supplier Solution to enable the Authority's personnel to readily locate such details.
The type of Personal Data being Processed	Name, corporate contact details (including email and phone number), job role and IP address.
The categories of Data Subjects	• Employees and Directors of companies that supply goods and services to the Authority and Service Recipients; and • Employees of the Authority and Service Recipients.
Location of Processing	The UK and the United States of America

APPENDIX 2

OVERVIEW OF SUPPLIER SOLUTION

[Bidder Note: This table will be completed using the information supplied as part of the Invitation to Tender Response.]

[Redacted for Publication]

SCHEDULE 4.2

COMMERCIALLY SENSITIVE INFORMATION

Issue No:	Summary of Change:
V0.1	Version for issue with ITT

I DEFINITIONS

i. In this Schedule, the definitions set out in Schedule 1 shall apply.

COMMERCIAL SENSITIVE INFORMATION

The information of a commercial sensitive nature which the Supplier has indicated to the Authority that, if disclosed by the Authority, would cause the Supplier significant commercial disadvantage or material financial loss is set out in Appendix 1.

APPENDIX 1

COMMERCIAL SENSITIVE INFORMATION

No.	Date	Item(s)	Duration of Confidentiality
1	September 17, 2022	Pricing	Indefinite
2	September 17, 2022	System Architecture	Indefinite
3	September 17, 2022	Any IT security policy or processes	Indefinite
4	September 17, 2022	All Product documentation, product specifications, IP, and related materials	Indefinite

SCHEDULE 5

SOFTWARE

Issue No:	Summary of Change:
V0.1	Version for issue with ITT

II. **DEFINITIONS**

ii. In this Schedule, the definitions set out in Schedule 1 shall apply.

4. **THE SOFTWARE**

4.1 The Software below is licensed to the Authority and the Service Recipients in accordance with Clauses 15 (*Intellectual Property Rights*) and 16 (*Licences Granted by the Supplier*).

4.2 The Parties agree that they will update this Schedule to record any Supplier Software or Third Party Software subsequently licensed by the Supplier or third parties for the purposes of the provision of the Services.

4.3 The Supplier warrants that the licence terms applicable to Third Party COTS Software:

4.3.1 are such as will enable the Authority and each Service Recipient to enjoy the full benefit of the Services and this Agreement; and

4.3.2 no fees, charges or expenses of any kind shall be due from the Authority or any Service Recipient in respect of the Third Party COTS Software other than the Charges payable to the Supplier under this Agreement,

and the Supplier acknowledges that it shall not be excused from performing any of its obligations or meeting any timeframes under this Agreement due to an act or omission of the relevant licensor of the Third Party COTS Software or any defect in the Third Party COTS Software.

[Redacted for Publication]

APPENDIX 6

FORM OF LETTER RE SUB-LICENSING OF SUPPLIER COTS SOFTWARE AND SUPPLIER COTS BACKGROUND IPRS

[Supplier letterhead]

[insert Authority name and address]

[Date]

Dear Sirs

LICENCES FOR SUPPLIER COTS SOFTWARE AND SUPPLIER COTS BACKGROUND IPRs

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 16.2.2] of the Agreement we confirm that:-

5. the Authority is licensed by the Supplier to use the Supplier COTS Software and Supplier COTS 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

6. notwithstanding any provision to the contrary in the Licences, it is agreed that the Authority may sub-license, assign and novate the Supplier COTS Software and Supplier COTS Background IPRs as referred to in [Clause 16.2.2] of the Agreement.

Yours faithfully

Signed:-

On behalf of [name of the Supplier]

APPENDIX 7

FORM OF CONFIDENTIALITY UNDERTAKING CONFIDENTIALITY AGREEMENT

THIS AGREEMENT IS MADE ON [DATE] 20

BETWEEN:-

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

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

WHEREAS:-

(A) *[insert name of Authority]* (the "**Authority**") 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 Authority.

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

(C) It is a requirement of the Contract that, before the Authority 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:-

7. **INTERPRETATION**

7.1 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 Authority 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 Authority pursuant to or in connection with the Sub-licence

(c) other Information provided by the Authority 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:-

(i) was in in the possession of the Sub-licensee without obligation of confidentiality prior to its disclosure by the Authority

(ii) the Sub-licensee obtained on a non-confidential basis from a third party who is not, to the Sub-licensee's knowledge or belief, bound by a confidentiality agreement with the Supplier or otherwise prohibited from disclosing the information to the Sub-licensee

(iii) 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

(iv) 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) and

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

7.2 In this Agreement:-

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

7.2.2 the singular includes the plural and vice versa;

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

7.2.4 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;

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

7.2.6 references to Clauses are to Clauses of this Agreement.

8. **CONFIDENTIALITY OBLIGATIONS**

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

8.1 treat all Confidential Information as secret and confidential;

8.2 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);

8.3 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;

8.4 not transfer any of the Confidential Information outside the United Kingdom and the European Union;

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

8.6 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

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

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

8.7.2 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

8.7.3 make no further use of any Confidential Information.

9. PERMITTED DISCLOSURES

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

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

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

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

9.2 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.

9.3 Before making a disclosure pursuant to Clause 1.2, the Sub-licensee shall, if the circumstances permit:-

9.3.1 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

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

10. GENERAL

10.1 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.

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

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

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

10.2.3 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.

10.3 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.

10.4 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.

10.5 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).

10.6 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.

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

10.8 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.

11. NOTICES

11.1 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 0.

11.2 Any Notice:-

11.2.1 if to be given to the Supplier shall be sent to:-

[Address]

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

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

[Name of Organisation]

[Address]

Attention: [ ]

12. **GOVERNING LAW**

12.1 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.

12.2 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 page 1.

Signed by [NAME OF SUPPLIER]
acting by

…… ……
Full Name [(Position)] Signature of [Position]

Signed for and on behalf of [NAME OF SUB-LICENSEE]
acting by

…… ……
Full Name [(Position)] Signature of [Position]

SCHEDULE 6.1

IMPLEMENTATION PLAN

Issue No:	Summary of Change:
V0.1	Version for issue with Tender Pack

13. **INTRODUCTION**

13.1 This Schedule: -

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

13.1.2 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.

14. **OUTLINE IMPLEMENTATION PLAN**

14.1 The Outline Implementation Plan is set out in Appendix 7.

14.2 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 27 (*Authority Cause*)).

15. **APPROVAL OF THE DETAILED IMPLEMENTATION PLAN**

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

15.2 The Supplier shall ensure that the draft Detailed Implementation Plan: -

15.2.1 incorporates all the Milestones and Milestone Dates set out in the Outline Implementation Plan.

15.2.2 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 for bespoke services only..

(b) the completion of the configuration phase.

(c) the completion of any Testing to be undertaken in accordance with Schedule 6.2 (*Milestone Achievement Procedure*).

(d) the completion of data migration and

(e) training and roll-out activities.

15.2.3 clearly outlines all the steps required to Achieve each of the Milestones together with a high-level plan for the rest of the programme, in conformity with the Authority Requirements;

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

15.2.5 is produced using a software tool as specified by the Supplier,

15.3 Prior to the submission of the draft Detailed Implementation Plan to the Authority in accordance with paragraph 1.2, the Authority shall have the right: -

15.3.1 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.

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

15.4 Following receipt of the draft Detailed Implementation Plan from the Supplier, the Authority shall: -

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

15.4.2 notify the Supplier in writing that it approves or rejects the draft Detailed Implementation Plan no later than ten (10) Working Days after the date on which the draft Detailed Implementation Plan is first delivered to the Authority.

15.5 If the Authority rejects the draft Detailed Implementation Plan: -

15.5.1 the Authority shall inform the Supplier in writing of its reasons for its rejection; and

15.5.2 the Supplier shall then revise the draft Detailed Implementation Plan (taking reasonable account of the Authority's comments) and shall re-submit a revised draft Detailed Implementation Plan to the Authority for the Authority's approval within ten (10) Working Days of the date of the Authority's notice of rejection. The provisions of paragraph 0 and this paragraph 1.1.1 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.

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

16. UPDATES TO AND MAINTENANCE OF THE DETAILED IMPLEMENTATION PLAN

16.1 Following the approval of the Detailed Implementation Plan by the Authority: -

16.1.1 the Supplier shall submit an updated Detailed Implementation Plan to the Authority every month starting one (1) month from the Effective Date.

16.1.2 without prejudice to paragraph 1.4, the Authority 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 Authority within ten (10) Working Days of receiving such a request from the Authority (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);

16.1.3 any revised Detailed Implementation Plan shall (subject to paragraph 0) be submitted by the Supplier for approval in accordance with the procedure set out in paragraph 3.1; and

16.1.4 the Supplier's performance against the Implementation Plan shall be monitored at Service, System Management and Performance Review Meetings (as defined in Schedule 8.1 (*Governance*)) and, where appropriate, the Joint Implementation Board (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 Authority not less than five (5) Working Days in advance of each meeting.

16.2 Save for any amendments which are of a type identified and notified by the Authority (at the Authority's discretion) to the Supplier in writing as not requiring approval, any amendments to the Detailed Implementation Plan which are: -

16.2.1 material, shall be subject to the Change Control Procedure provided that: -

(a) 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

(b) in no circumstances shall the Supplier be entitled to alter or request an alteration to any Milestone Date except in accordance with Clause 27 (*Authority Cause*); and

16.2.2 non-material shall be subject to the Document Change Procedure.

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

17. RELATED IMPLEMENTATION PLANS

17.1 The Supplier acknowledges that the Detailed Implementation Plan may need to be consistent with and interoperate with, the implementation plans of the Authority and other third-party suppliers to the Authority including those of any Other Supplier as determined by the Authority (each a "**Related Implementation Plan**").

17.2 The Supplier shall (at no cost to the Authority) cooperate with the Authority and other third party suppliers to the Authority (including the Other Suppliers (which may include attendance at workshops) and promptly provide to such third parties all documentation, data, information or other assistance reasonably requested by the Authority in relation to: -

17.2.1 the preparation of the Detailed Implementation Plan and Related Implementation Plans; and

17.2.2 the alignment of the Detailed Implementation Plan with the Related Implementation Plans (and vice versa).

18. GOVERNMENT REVIEWS

The Supplier acknowledges that the Services may be subject to Government review 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.

APPENDIX 8

OUTLINE IMPLEMENTATION PLAN – MAIN SYSTEM

*All Milestone Dates are subject to the contract Effective Date and acceptance of the Project Plan submitted by the Bidder to the Project Victory Board. The milestones dates contained in this schedule should therefore be considered indicative only.

MAIN SYSTEM IMPLEMENTATION				
Milestone	Deliverables (list showing all Deliverables (and associated tasks) required for each Milestone)	Start date	End date	Duration (Working Days)
1.1 Mobilisation Complete	Project Plan Risk and Issues Management Plan and Registers Service Continuity Plan Detailed Implementation Plan Service Management Plan Outline Contract Exit Plan	20 September 2022	12 October 2022	17
1.2 Full Development / Configuration Complete	System developed and configured in accordance with Authority requirements and ready to commence testing Existing (Sellafield) supply chain tiering data transferred to system Updated Risk and Issues Management Plan and Registers Updated Disaster Recovery Plan	13 October 2022	10 November 2022	21
1.3 Testing Complete	Updated Risk and Issues Management Plan Updated Project Plan Updated Disaster Recovery Plan Training Plan Drafted Reporting provided in accordance with Schedule 8.4. Defects Log System Testing Report · Integration Testing across the Project Victory systems · Functional Requirement Testing · Destructive Testing · Penetration Testing · Fault Injection Testing	11 November 2022	15 December 2022	25

	· Resolution of Defects and re-test · Final Inspection and Testing Report, with Authority approval			
	User Acceptance Testing Report · Test Scripts provided to testers · User Acceptance Testing · Resolution of Defects and re-test · Final UAT Report			
1.4 Training Documentation Complete	Training documentation complete reviewed and signed off Updated Risk and Issues Log	16 December 2022	22 December 2022	5
1.5 User Readiness for Service	Training Plan developed Updated Risk and Issues Log Detailed Contract Exit Plan Training Plan delivered Supplier Helpdesk Trained Go Live helpdesk support provided	03 January 2023	16 January 2023	10
1.6 Implementation Complete	System live and all businesses migrated to system Service Delivery Reports Risk and Issues Log updated Post Implementation Report and Lessons Learnt Review	17 January 2023	13 February 2023	20
1.7 Contract Exit	Updated Contract Exit Plan covering data/information management and data migration. The updated Contract Exit Plan is to reflect the current data/information held in the System and any additional operational considerations not previously reflected in the Contract Exit Plan at Milestone 1.5. Exit Plan delivered Post Contract Exit Report	From Commencement Date	20/09/2026* Indicative based on 4 year duration. If extension options used	

			20/09/2028 or 20/09/2030.	

APPENDIX B

OUTLINE IMPLEMENTATION PLAN – LOT D SYSTEM INTERFACES (REFER TO VOLUME 5 FOR FULL DETAIL)

INTERFACE IMPLEMENTATION				
Milestone	Deliverables (list showing all Deliverables (and associated tasks) required for each Milestone)	Start date	End date	Duration (Working Days)
2.1 Interface Mobilisation Complete	Project Plan Risk and Issues Management Plan and Registers Disaster Recovery Plan Detailed Implementation Plan developed with interface providers (as per Volume 3, Volume 5 and Volume 7) Detailed Implementation Plan developed with interface providers (as per Volume 3, Volume 5 and Volume 7) Updated Contract Exit Plan (refer to Milestones 1.5 and 1.7) covering Interface Decommissioning, data / management (and data migration as required)	*Dates to be agreed between NDA, Supplier and interface providers		
2.2 Interface Full Development / Configuration Complete	Interface developed and configured in accordance with Authority requirements and ready to commence testing Interface and User Acceptance Testing Strategy Updated Risk and Issues Management Plan and Registers Updated Disaster Recovery Plan	*Dates to be agreed between NDA, Supplier and interface providers		
2.3 Interface Testing Complete	Updated Risk and Issues Management Plan Updated Project Plan Updated Disaster Recovery Plan Reporting provided in accordance with Schedule 8.4. Defects Log System Testing Report · Integration Testing across the modules of the Lot A system · Functional Requirement Testing · Destructive Testing	*Dates to be agreed between NDA, Supplier and interface providers		

	· Penetration Testing · Fault Injection Testing · Resolution of Defects and re-test · Final Inspection and Testing Report, with Authority approval User Acceptance Testing Report · Test Scripts provided to testers · User Acceptance Testing · Resolution of Defects and re-test · Final UAT Report	
2.4 Interface Implementation Complete	Interface 'switched on' Post Implementation Report and Lessons Learnt Review	*Dates to be agreed between NDA, Supplier and interface providers

SCHEDULE 6.2

MILESTONE ACHIEVEMENT PROCEDURE

Issue No:	**Summary of Change:**
V0.1	Version for issue with ITT

DEFINITIONS

18.1 In this Schedule, the definitions set out in Schedule 1 shall apply.

19. **SCOPE**

19.1 This Schedule sets out the principles and procedures in respect of Achievement by the Supplier of a Milestone.

19.2 In respect of each Milestone the Milestone Achievement Procedure shall include:-

19.2.1 conducting any Testing (where required in accordance with the Implementation Plan or any future Change Authorisation Note (as applicable));

19.2.2 demonstrating successful completion of Achievement Criteria; and

19.2.3 resolution of a failure to meet any Acceptance Criteria (if any).

19.3 This Schedule will operate alongside:-

19.3.1 for Implementation, Schedule 6.1 (*Implementation*) and the Implementation Plan shall set out the Achievement Criteria (including details of any Testing and supporting evidence required) for all Milestones to be Achieved during Implementation; and

19.3.2 for future Projects, Schedule 8.2 (*Change Control Procedure*) and the applicable Change Authorisation Note shall set out the Achievement Criteria (including details of any Testing and supporting evidence required) for all Milestones to be Achieved during the relevant Project.

20. **RISK**

20.1 Unless otherwise agreed in writing by the Authority, Achievement of any Milestone shall only occur when all Achievement Criteria relating to it have been met and the Authority has issued a Milestone Achievement Certificate on an unconditional basis in accordance with this Schedule.

20.2 The issue of a Milestone Achievement Certificate and/or a conditional Milestone Achievement Certificate shall not:-

20.2.1 operate to transfer any risk that the relevant Milestone (including any component items of that Milestone, such as a Deliverable) is complete or will meet and/or satisfy the Authority's requirements for that Milestone; or

20.2.2 affect the Authority's right subsequently to reject any Milestone (including any component items, such as a Deliverable) to which the Milestone Achievement Certificate relates.

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

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

20.3.2 the Services are implemented in accordance with this Agreement; and

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

21. ISSUE OF A MILESTONE ACHIEVEMENT CERTIFICATE

21.1 The Supplier shall deliver to the Authority the documentary evidence agreed to be produced as part of the Implementation Plan or Change Authorisation Note (as applicable), together with any supporting information reasonably required, in sufficient time to Achieve a Milestone on or before the Milestone Date for that Milestone.

21.2 Within ten (10) Working Days of receipt of the documentary evidence from the Supplier in accordance with paragraph 21.1 (or such other period as may be agreed), the Authority shall notify the Supplier whether the Supplier has successfully completed, to the reasonable satisfaction of the Authority, the applicable Achievement Criteria and the Milestone is therefore Achieved or not. Where:-

21.2.1 the Milestone is Achieved, the Authority shall issue a Milestone Achievement Certificate in respect of the given Milestone; or

21.2.2 the Milestone is not Achieved, the Authority shall promptly issue a report to the Supplier setting out the reasons for the relevant Milestone not being Achieved. Thereafter, where required by the Authority, the Supplier shall re-submit the documentary evidence together with any supporting information reasonably required as many times as is necessary until the Supplier has successfully completed, to the reasonable satisfaction of the Authority, the applicable Achievement Criteria (whereupon the Authority shall issue a Milestone Achievement Certificate).

21.3 The grant of a Milestone Achievement Certificate (where applicable and as identified in the relevant Implementation Plan or Change Authorisation Note) 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*).

21.4 Without prejudice to the Authority's other remedies, if the Supplier fails through its Default to Achieve a Milestone on or before the relevant Milestone Date in accordance with this Schedule such failure shall constitute a Notifiable Default by the Supplier for the purposes of Clause 26.1 (*Rectification Plan Process*).

21.5 Where the Authority notifies the Supplier that it does not consider that the Achievement Criteria for any Milestone have been met in accordance with paragraph 21.2.2, the Authority 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 Achievement Criteria in accordance with an agreed Rectification Plan provided that: -

21.5.1 any Rectification Plan shall be agreed before the issue of a conditional Milestone Achievement Certificate unless the Authority agrees otherwise (in which case the Supplier shall submit a Rectification Plan for approval by the Authority within ten (10) Working Days of receipt of the Authority's notice provided pursuant to paragraph 21.2.2); and

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

APPENDIX 9

MILESTONE ACHIEVEMENT CERTIFICATE

To: [**NAME OF SUPPLIER**]

FROM: [**NAME OF AUTHORITY**]

[**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 Authority] (the "**Authority**") 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 (Milestone Achievement Procedure)] of the Agreement.

[We confirm that all the Supplier has successfully completed the Achievement Criteria for Milestone [number] in accordance with the [Implementation Plan]OR[Change Authorisation Note]]*

OR

[This Milestone Achievement Certificate is granted pursuant to paragraph 21.221.5 of [Schedule 6.2 (Milestone Achievement Procedure)] of the Agreement on the condition that any Achievement Criteria not met (as determined by the Authority) 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 [Authority]

SCHEDULE 7.1

CHARGES AND INVOICING

Issue No:	**Summary of Change:**
V0.1	Version for issue with ITT

DEFINITIONS

i. In this Schedule, the definitions set out in Schedule 1 shall apply.

PART A

PRICING

1. **GENERAL**

1.1 This Schedule sets out the provisions relating to:-

1.1.1 the Charges applicable to the provision of the Services;

1.1.2 invoicing matters; and

1.1.3 other financial and economic matters relating to this Agreement.

1.2 The following Charges shall be payable by the Authority in accordance with this Agreement:-

1.2.1 Service Charges

1.2.2 Milestone Achievement Certificate Charges

1.2.3 Additional Service Charges;

1.2.4 Additional Development Charges;

1.2.5 the Termination Services Charges (as further described in Schedule 7.2).

2. **APPLICABLE PRICING MECHANISM**

2.1 Milestone Payments and Service Charges shall be calculated using the pricing mechanisms specified in **Error! Reference source not found.** and **Error! Reference source not found.** and on the basis of the rates and prices specified in **Error! Reference source not found.** as more particularly set out in this Schedule.

2.2 The pricing mechanisms set out in the tables in **Error! Reference source not found.**, **Error! Reference source not found.** and **Error! Reference source not found.** specify whether the pricing mechanism is:-

2.2.1 "**Fixed Price**", in which case the provisions of paragraph 4 shall apply;

2.2.2 **"Volume Based**", in which case the provisions of paragraph 1.2 shall apply;

2.2.3 **"Time Based"**, in which case the provisions of paragraph 3 shall apply.

3. TIME SERVICE CHARGES

3.1 The Day Rates set out in the Rate Card **Error! Reference source not found.** of **Error! Reference source not found.** shall be used to calculate the Time Service Charges due to the Supplier. The Supplier shall not be entitled to include any uplift for risks or contingencies within its day rates.

3.2 The Rate Card applies to Additional Services only.

3.3 The Authority shall request the Supplier to provide a quote for any Additional Services required. The Supplier shall provide a written quote to the Authority for written approval by the Authority prior to the commencement of any Additional Services.

3.4 The Supplier shall keep records of the Man Days properly worked by Supplier Personnel (in the form of timesheets) and expenses incurred and submit a summary of the relevant records with each invoice.

3.5 The Standard Rate Charges set out in the Development Charges **Error! Reference source not found.** of **Error! Reference source not found.** shall be used to calculate the Fixed Prices due to the Supplier for Additional Development. The Supplier shall not be entitled to include any uplift for risks or contingencies within its Standard Rate Charges.

3.6 The Standard Rate Charges apply to Additional Development Services only.

3.7 The Authority shall request the Supplier to provide a quote for any Additional Development required. The Supplier shall provide a written quote to the Authority for written approval by the Authority prior to the commencement of any Additional Development.

3.8 The Authority's request for quote and subsequent Work Order shall include a specification of the Additional Development required and Acceptance Criteria to meet to initiate an Additional Milestone payment. The Acceptance Criteria shall have the meaning of the quality criteria the Supplier is required to fulfil before any payment is made to the Supplier for the Additional Development rendered.

3.9 On fulfilment of the Acceptance Criteria, the Authority shall issue a Milestone Achievement Certificate to the Supplier.

3.10 Charges calculated by reference to a Time Service Charge mechanism shall not be subject to increase by way of Indexation.

4. FIXED PRICE MILESTONE PAYMENTS

4.1 The Fixed Price Milestone Payments set out in **Error! Reference source not found.**, **Error! Reference source not found.** and Appendix 4 shall be used to calculate the Fixed Price Milestone Payments due to the Supplier. The Supplier shall not be entitled to include any uplift for risks or contingencies unless the Supplier can demonstrate any incurred costs were caused by the Authority in accordance with paragraph 7.

4.2 Where **Error! Reference source not found.** indicates that a Milestone Payment or Service Charge is to be calculated by reference to a Fixed Price pricing mechanism, the relevant Charge shall be the amount set out against that Charge in **Error! Reference source not found.**.

4.3 Charges calculated by reference to a Fixed Price pricing mechanism shall be subject to increase by way of Indexation.

5. VOLUME BASED SERVICE CHARGES

5.1 Where **Error! Reference source not found.** indicates that a Service Charge is to be calculated by reference to a Volume Based pricing mechanism, the relevant Charges shall be calculated on the basis of the unit costs set out against that Service Charge in **Error! Reference source not found.**.

5.2 In the event that the volume of any Services that are to be calculated by reference to a Volume Based pricing mechanism fall outside the relevant volume bands set out against that Service Charge **Error! Reference source not found.**, the relevant Service Charges shall be calculated in accordance with the Schedule 8.2 (*Change Control Procedure*).

5.3 The Charges per unit set out in **Error! Reference source not found.** shall be subject to annual Indexation.

6. REIMBURSABLE EXPENSES

6.1 Where:-

6.1.1 Services are to be charged using the Time pricing mechanism; and

6.1.2 the Authority so agrees in writing, the Supplier shall be entitled to be reimbursed by the Authority for Reimbursable Expenses (in addition to being paid the relevant Charges), provided that such Reimbursable Expenses are reasonable and supported by Supporting Documentation.

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

6.3 Except as expressly set out in paragraph 6.1, 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 Authority to the Supplier in respect of such performance, including in respect of matters such as:-

6.3.1 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

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

PART B – [NOT USED]

PART C

ADJUSTMENTS TO THE CHARGES

7. PAYMENTS FOR DELAYS DUE TO AUTHORITY CAUSE

7.1 If the Supplier is entitled in accordance with Clause 27 (*Authority Cause*) to compensation for failure to Achieve a Milestone by its Milestone Date [as agreed with the Authority], then, subject always to Clause 25 (*Limitations on Liability*), such compensation shall be determined in accordance with the following principles:-

7.1.1 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 Authority Cause; and

(b) is, has been, or will be unable to mitigate, having complied with its obligations under Clause 31.1 (*Authority Cause*),

7.2 The Supplier shall provide the Authority with any information the Authority may require in order to assess the validity of the Supplier's claim to compensation.

8. SERVICE CREDITS

8.1 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*).

8.2 For each Service Period:-

8.2.1 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 five (5) % deduction in the Service Charges; and

8.2.2 the total Service Credits applicable for the Service Period shall be calculated in accordance with the following formula:-

SC = TSP X 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 5% per Service Point; and

AC is the total Services Charges payable for the relevant Service Period (prior to deduction of applicable Service Credits).

8.3 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.

8.4 Service Credits shall be shown as a deduction from the amount due from the Authority to the Supplier in the invoice for the Service Period immediately succeeding the Service Period to which they relate.

9. CHANGES TO CHARGES

9.1 Any Changes to the Charges (including the introduction of any new Charges) shall be developed and agreed by the Parties in accordance with Schedule 8.2 (*Change Control Procedure)*.

9.2 The Authority may request that any Impact Assessment presents Charges without Indexation for the purposes of comparison.

10. INDEXATION

10.1 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 paragraphs 4.3 and 5.3 to reflect the effects of inflation.

10.2 Where Indexation applies, the relevant adjustment shall be:-

10.2.1 applied on the first day of the third April following the Effective Date and on the first day of April in each subsequent year (each such date an "**adjustment date**"); and

10.2.2 determined by multiplying the relevant amount or sum by the percentage increase or changes in the Consumer Price Index published for the twelve (12) months ended on the 31 January immediately preceding the relevant adjustment date.

10.3 Except as set out in this paragraphs 4.3 and 5.3, 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.

PART D – [NOT USED]

PART E

INVOICING AND PAYMENT TERMS

11. SUPPLIER INVOICES

11.1 The Authority shall accept for processing any electronic invoice that complies with the European Standard, provided that it is valid and undisputed.

11.2 If the Supplier proposes to submit for payment an invoice that does not comply with the European Standard, the Supplier shall comply with the requirements of the Authority's e-invoicing system. In the alternative, the Supplier shall:-

11.2.1 prepare and provide to the Authority for approval of the format a template invoice within ten (10) Working Days of the Effective Date which shall include, as a minimum, the details set out in paragraph 11.3 together with such other information as the Authority may reasonably require to assess whether the Charges that will be detailed therein are properly payable; and

11.2.2 make such amendments as may be reasonably required by the Authority if the template invoice outlined in paragraph 11.3 is not approved by the Authority.

11.3 The Supplier shall ensure that each invoice contains the following information:-

11.3.1 the date of the invoice;

11.3.2 a unique invoice number;

11.3.3 the Service Period or other period(s) to which the relevant Charge(s) relate;

11.3.4 the correct reference for this Agreement;

11.3.5 the correct reference number of the purchase order to which it relates (if any);

11.3.6 the dates between which the Services subject of each of the Charges detailed on the invoice were provided;

11.3.7 a description of the Services;

11.3.8 the pricing mechanism used to calculate the Charges (such a, Fixed Price, Time etc);

11.3.9 any payments due in respect of Achievement of a Milestone, including the Milestone Achievement Certificate number for each relevant Milestone;

11.3.10 the total Charges gross and net of any applicable deductions and, separately, the amount of any Reimbursable Expenses properly chargeable to the Authority under the terms of this Agreement, and, separately, any VAT or other sales tax payable in respect of each of the same;

11.3.11 details of any Service Credits or Delay Payments or similar deductions that shall apply to the Charges detailed on the invoice;

11.3.12 for bespoke service, reference to any reports required by the Authority 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 Authority, then to any such reports as are validated by the Authority in respect of the Services);

11.3.13 a contact name and telephone number of a responsible person in the Supplier's finance department in the event of administrative queries;

11.3.14 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

11.3.15 where the Services have been structured into separate Service lines, the information at paragraph 11.3.1 to 5.8 (inclusive) shall be broken down in each invoice per Service line.

11.4 The Supplier shall invoice the Authority in respect of Services in accordance with the requirements of Part B.

11.5 Each invoice shall at all times be accompanied by Supporting Documentation. Any assessment by the Authority as to what constitutes Supporting Documentation shall not be conclusive and the Supplier undertakes to provide to the Authority any other documentation reasonably required by the Authority from time to time to substantiate an invoice.

11.6 The Supplier shall submit all agreed invoices to the Authority electronically by emailing:-

apqueries@nda.gov.uk

with a copy to such other person and at such place as the Authority may notify to the Supplier from time to time.

11.7 All Supplier invoices shall be expressed in sterling or such other currency as shall be permitted by the Authority in writing.

11.8 The Authority 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 Authority's requirements set out in this Part 5, the Authority shall promptly return the disputed invoice to the Supplier and the Supplier shall promptly issue a replacement invoice which shall comply with such requirements.

11.9 If the Authority fails to consider and verify an invoice in accordance with paragraphs 11.4 and 11.8, the invoice shall be regarded as valid and undisputed after a reasonable time has passed.

11.10 The Supplier shall ensure that all Supplier invoices do not reference any terms and conditions other than this Agreement. Where a Supplier invoice references any other terms and conditions, such Supplier invoice will not be valid and the Supplier shall promptly issue a replacement invoice which complies with this requirement.

11.11 The supplier shall provide

12. PAYMENT TERMS

12.1 Subject to the relevant provisions of this Schedule, the Authority shall make payment to the Supplier within thirty (30) days of verifying that the invoice is valid and undisputed.

12.2 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.

12.3 Licence fees to be paid quarterly in advance equating to 25% of the total licence fee charges in each contract year as referenced at appendix 1. First payment to be made on receipt of the invoice in accordance with paragraph 12.1 with three further payments made every three months in each contract year.

[Redacted for Publication]

SCHEDULE 7.2

PAYMENTS ON TERMINATION

Issue No:	Summary of Change:
V0.1	Version for issue with ITT

1. **DEFINITIONS**

1.1 In this Schedule, the definitions set out in Schedule 1 shall apply.

2. **TERMINATION PAYMENT**

The termination payment payable pursuant to Clause 30.3 (*Payments by the Authority*) shall be an amount equal to the aggregate of the Breakage Costs Payment and the Unrecovered Payment (the "**Termination Payment**").

3. **BREAKAGE COSTS PAYMENT**

3.1 The Supplier may be entitled to 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;

3.1.6 is not due to the occurrence of any Supplier Termination Event defined in Schedule 1.

4. **LIMITATION ON TERMINATION PAYMENT**

4.1 Subject to paragraph 4.3, the Termination Payment shall not exceed the lower of:

4.1.1 the aggregate of the relevant limits set out in Appendix 1 for the Breakage Costs Payment and the Unrecovered Payment; and

4.1.2 100% of the estimate of the Termination Payment set out in any relevant Termination Estimate.

4.2 The Breakage Costs Payment shall not exceed the lower of:-

4.2.1 the relevant limit set out in Appendix 10; and

4.2.2 100% of the estimate for the Breakage Costs Payment set out in any relevant Termination Estimate.

4.3 The Unrecovered Payment shall not exceed the lowest of:-

4.3.1 the relevant limit set out in Appendix 10;

4.3.2 100% of the estimate of the Unrecovered Payment set out in any relevant Termination Estimate; and

4.3.3 the Charges that but for the termination of this Agreement would have been payable by the Authority after the Termination Date in accordance with Schedule 7.1 (*Charges and Invoicing*) as forecast in the Financial Model.

5. MITIGATION OF THE TERMINATION PAYMENT

5.1 The Supplier agrees to use all reasonable endeavours to minimise and mitigate the Termination Payment by:-

5.1.1 the appropriation of Assets, employees and resources for other purposes;

5.1.2 at the Authority's request, assigning any Third Party Contracts and Sub-contracts to the Authority or a third party acting on behalf of the Authority; and

5.1.3 in relation Third Party Contracts and Sub-contract that are not to be assigned to the Authority or to another third party, terminating those contracts at the earliest possible date without breach or where contractually permitted.

5.2 If Assets, employees and resources can be used by the Supplier for other purposes, then there shall be an equitable reduction in the Termination Payment payable by the Authority 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*).

6. FULL AND FINAL SETTLEMENT

Any Termination 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 Authority pursuant to Clause 31.1.1 (*Termination by the Authority)* or termination by the Supplier pursuant to Clause 31.3.1 (*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

All sums due under this Schedule shall be payable by the Authority to the Supplier in accordance with the payment terms set out in Schedule 7.1 (*Charges and Invoicing*).

8. SET OFF

The Authority 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 Authority 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 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

10.1 The Authority 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 that would be payable by the Authority 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 Authority may reasonably require;

10.2.3 [full particulars of the estimated Unrecovered Payment and appropriate supporting documentation;] and

10.2.4 state the period for which that Termination Estimate remains valid, which shall be not less than sixty (60) 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 Authority to terminate this Agreement.

10.4 If the Authority 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 Authority.

APPENDIX 10

MAXIMUM PAYMENTS ON TERMINATION

Except for Termination for Convenience, the table below sets out, by Contract Year, the maximum amount of the Unrecovered Payment, Breakage Costs Payment that the Authority shall be liable to pay to the Supplier pursuant to this Agreement:-

Termination Date	Maximum Unrecovered Payment	Maximum Breakage Costs Payment
Anytime in the first Contract Year once the Milestone Achievement Certificate has been issued for Milestone 1.5 System Implementation Complete as defined in Schedule 6.1 (*Implementation Pla*n)	One month's contract value = Annual Contract Value divided by twelve (12) Plus, Any unpaid Service Charges due issue of a Milestone Achievement Certificate.	One and a half (1.5) years' Annual Contract Value
Anytime in the second Contract Year		One (1) year's Annual Contract Value
Anytime in the third Contract Year		Six months (6) Annual Contract Value

FOR TERMINATION FOR CONVENIENCE AUTHORITY WILL PAY SUPPLIER FOR THE ANNUAL CONTRACT VALUE LESS ANY AMOUNTS PAID FOR THAT CONTRACT YEAR.

SCHEDULE 7.5

FINANCIAL REPORTS AND AUDIT RIGHTS

Issue No:	Summary of Change:
V0.1	Version for issue with ITT

I. **DEFINITIONS**

i. In this Schedule, the definitions set out in Schedule 1 shall apply.

1. **FINANCIAL TRANSPARENCY OBJECTIVES**

1.1 The Supplier shall collaborate with the Authority to achieve the following objectives:-

Understanding the Charges

1.1.1 for both Parties to be able to understand the Financial Model and Cost forecasts and to have confidence that these are based on justifiable numbers and appropriate forecasting techniques;

Agreeing the impact of Change

1.1.2 for both Parties to agree the quantitative impact of any Changes that affect ongoing costs and to identify how these could be mitigated and/or reflected in the Supplier's Charges;

1.1.3 for both Parties to be able to review, address issues with and re-forecast progress in relation to the provision of the Services;

Continuous improvement

1.1.4 for the Parties to challenge each other with ideas for efficiency and improvements;

1.1.5 to enable the Authority to demonstrate that it is achieving value for money for the tax payer relative to current market prices, and

(together the "**Financial Transparency Objectives**")

2. **AUDIT RIGHTS**

2.1 The Authority, acting by itself or through its Audit Agents, shall have the right during the Term, any Termination Assistance Period and for a period of eighteen (18) months after the later of the end of the Term and the end of any Termination Assistance Period, to assess compliance by the Supplier of the Supplier's obligations under this Agreement, including for the following purposes:-

2.1.1 to review the Supplier's activities in connection with, and performance in respect of, this Agreement (including the IT Environment (or any part of it) and the wider service delivery environment (or any part of it)) and to verify the Supplier's compliance with this Agreement and applicable Law (including the Data Protection Legislation);

2.1.2 to verify the accuracy of the Charges and Costs (including the amounts paid to all Sub-contractors and any third party suppliers) and any other amounts payable by the Authority

under this Agreement (and proposed or actual variations to such Charges, Costs and payments) which shall include the verification of any supporting documentation in respect of such Charges and Costs;

2.1.3 to identify or investigate actual or suspected fraud, impropriety or accounting mistakes, any circumstances which may impact upon the financial stability of the Supplier and/or any of the Supplier Group or their ability to provide the Services or any breach or threatened breach of security and in these circumstances the Authority shall have no obligation to inform the Supplier of the purpose or objective of its investigations;

2.14 to obtain such information as is necessary to fulfil the Authority's obligations to supply information for parliamentary, ministerial, judicial or administrative purposes including the supply of information to the Comptroller and Auditor General;

2.1.5 to review all information required to be kept by the Supplier pursuant to this Agreement;

2.1.6 to verify the accuracy and completeness of any Management Information delivered or required by this Agreement;

2.1.7 to review the integrity, confidentiality and security of the information required to be kept by the Supplier pursuant to this Agreement (including the Authority Data); and

2.1.8 to carry out the Authority's internal and statutory audits and to prepare, examine and/or certify the Authority's annual and interim reports and accounts.

2.2 Except where an audit is imposed on the Authority by a regulatory body or where the Authority has reasonable grounds for believing that the Supplier has not complied with its obligations under this Agreement, the Authority may not conduct an audit of the Supplier more than twice in any Contract Year. For the purposes of this paragraph 2.2 the final Contract Year shall end on the last date of the Termination Assistance Period..

2.3 Nothing in this Agreement shall prevent or restrict the rights of the Comptroller and/or Auditor General and/or their representatives from carrying out an audit, examination or investigation of the Supplier for the purposes of and pursuant to applicable Law.

3. CONDUCT OF AUDITS

3.1 The Authority shall during each audit comply with those security, sites, systems and facilities operating procedures of the Supplier that the Authority deems reasonable and use its reasonable endeavours to ensure that the conduct of each audit does not unreasonably disrupt the Supplier or delay the provision of the Services.

3.2 Subject to the Authority's obligations of confidentiality, the Supplier shall on demand provide the Authority and the Audit Agents with all reasonable co-operation and assistance (and shall procure such co-operation and assistance from its Sub-contractors) in relation to each audit, including:-

3.2.1 all information requested by the Authority within the permitted scope of the audit; and

3.2.2 reasonable access to any Supplier Personnel and required financial information.;

3.3 Where appropriate, the Authority shall discuss the outcome of the audit with the Supplier. In such circumstances, the Supplier shall maintain records of the findings together with details of any corrective action taken as a result of such findings.

3.4 The Authority shall bear costs and expenses incurred in respect of compliance with their obligations under this paragraph 3, unless the audit identifies a material Default by the Supplier in which case the Supplier shall reimburse the Authority for all the Authority's reasonable costs incurred in connection with the audit.

4. RESPONSE TO AUDITS

4.1 If an audit undertaken pursuant to paragraph 2 identifies that:-

4.1.1 the Supplier has committed a Default, the Authority may (without prejudice to any rights and remedies the Authority may have) require the Supplier to correct such Default as soon as reasonably practicable and, if such Default constitutes a Notifiable Default, to comply with the Rectification Plan Process;

4.1.2 there is an error in a Financial Report, the Supplier shall promptly rectify the error;

4.1.3 the Authority has overpaid any Charges, the Supplier shall pay to the Authority:-

(a) the amount overpaid (excluding any interest on the amount overpaid incurred in accordance with the terms of this Agreement); and

(b) the reasonable costs incurred by the Authority in undertaking the audit and the Authority may exercise its right to deduct such amount from the Charges if it prefers; and

4.1.4 the Authority has underpaid any Charges, subject to the terms of payment set out in this Agreement, the Authority shall pay to the Supplier the amount underpaid as identified in the audit report and on provision by the Supplier of all reasonable evidence required by the Authority in connection to such underpaid amount (excluding any interest that may have accrued up to the date of payment).

SCHEDULE 8.1

GOVERNANCE

Issue No:	Summary of Change:
V0.1	Version for issue with ITT

I. DEFINITIONS

i. In this Schedule, the definitions set out in Schedule 1 shall apply.

1. MANAGEMENT OF THE SERVICES

1.1 The Supplier and the Authority shall each appoint a project manager for the purposes of this Agreement through whom the Services shall be managed on a day-to-day basis.

1.2 Both Parties shall ensure that appropriate resource is made available on a regular basis such that the aims, objectives and specific provisions of this Agreement can be fully realised.

2. BOARDS

Establishment and structure of the Boards

2.1 The Boards shall be established by the Authority for the purposes of this Agreement on which both the Supplier and the Authority shall be represented.

2.2 In relation to each Board, the:-

2.2.1 Authority Board Members;

2.2.2 Supplier Board Members;

2.2.3 frequency that the Board shall meet (unless otherwise agreed between the Parties);

2.2.4 location of the Board's meetings; and

2.2.5 planned start date by which the Board shall be established, shall be as set out in Appendix 11.

2.3 In the event that either Party wishes to replace any of its appointed Board Members, that Party shall notify the other in writing of the proposed change for agreement by the other Party (such agreement not to be unreasonably withheld or delayed). Notwithstanding the foregoing it is intended that each Authority Board Member has at all times a counterpart Supplier Board Member of equivalent seniority and expertise.

Board meetings

2.4 Each Party shall ensure that its Board Members shall make all reasonable efforts to attend Board meetings at which that Board Member's attendance is required. If any Board Member is not able to attend a Board meeting, that person shall use all reasonable endeavours to ensure that:-

2.4.1 a delegate attends the relevant Board meeting in his/her place who (wherever possible) is properly briefed and prepared; and

2.4.2 that he/she is debriefed by such delegate after the Board Meeting.

2.5 A chairperson shall be appointed by the Authority for each Board as identified in Appendix 11. The chairperson shall be responsible for:-

2.5.1 scheduling Board meetings;

2.5.2 setting the agenda for Board meetings and circulating to all attendees in advance of such meeting;

2.5.3 chairing the Board meetings;

2.5.4 monitoring the progress of any follow up tasks and activities agreed to be carried out following Board meetings;

2.5.5 ensuring that minutes for Board meetings are recorded and disseminated electronically to the appropriate persons and to all Board meeting participants within seven Working Days after the Board meeting; and

2.5.6 facilitating the process or procedure by which any decision agreed at any Board meeting is given effect in the appropriate manner.

2.6 Board meetings shall be quorate as long as at least two representatives from each Party are present.

2.7 The Parties shall ensure, as far as reasonably practicable, that all Boards shall as soon as reasonably practicable resolve the issues and achieve the objectives placed before them. Each Party shall endeavour to ensure that Board Members are empowered to make relevant decisions or have access to empowered individuals for decisions to be made to achieve this.

3. ROLE OF THE JOINT IMPLEMENTATION BOARD

3.1 The Joint Implementation Board shall be responsible for the delivery of the implementation of the Services where an Automated Program Interface is required or specified, and shall:-

3.1.1 be accountable to the Commercial Systems Governance Board for comprehensive oversight of the Services and for the senior management of the operational relationship between the Parties;

3.1.2 report to the Commercial Systems Governance Board on significant issues requiring decision and resolution and on progress against the high level Implementation Plan;

3.1.3 receive reports from the Project Managers on matters such as issues relating to delivery of existing Services and performance against Performance Indicators, progress against the Implementation Plan and possible future developments;

3.1.4 review and report to the Commercial Systems Governance Board on service management, coordination of individual projects and any integration issues;

3.1.5 deal with the prioritisation of resources and the appointment of Project Managers on behalf of the Parties;

3.1.6 consider and resolve Disputes (including Disputes as to the cause of a Delay or the provision of the Services) in the first instance and if necessary, escalate the Dispute to the Commercial Systems Governance Board; and

3.1.7 develop operational/supplier relationships and develop and propose the relationship development strategy and ensure the implementation of the same.

3.2 The Joint Implementation Board may meet either separately with each System Supplier or with multiple Supplier representatives as mutually agreed to progress the Implementation Plan.

3.3 The Joint Implementation Board shall remain until the systems are live and handed over to the Authority in accordance with the Implementation Plan, after which point further development will be considered by the Supplier Forum (paragraph 6 below).

4. ROLE OF THE COMMERCIAL SYSTEMS GOVERNANCE BOARD

4.1 The Commercial Systems Governance Board shall:-

4.1.1 provide senior level guidance, leadership and strategy for the overall delivery of the Services;

4.1.2 be the point of escalation from the Joint Implementation Board; and

4.1.3 carry out the specific obligations attributed to it in paragraph 4.2.

4.2 The Commercial Systems Governance Board shall:-

4.2.1 act as a change control board for the development of the systems;

4.2.2 review reports on technology, service and other developments that offer potential for improving the benefit that either Party is receiving, in particular value for money;

4.2.3 maintain a log of development change proposals and prioritise them for progressing further and refer them to the Supplier Group to discuss and propose an approach;

4.2.4 for proposals agreed by the board to be progressed, obtain suitable costings and prepare business cases for the developments to be funded;

4.2.5 obtain the necessary approvals for business cases;

4.2.6 review and approve the final specifications for changes, liaising with the Supplier Forum to ensure best practice;

4.2.7 ensure that plans are put in place for the development and testing of proposals and that the required internal resource is made available in a timely way to facilitate this;

4.2.8 review the performance of the systems, receiving contract performance reports and reports from super-users and/or supplier helpdesks on common issues, and to manage the delivery of any action plans for the rectification of issues and fault;

4.2.9 review risk and issues logs for the systems, ensuring these are kept current and that new risks are added and obsolete ones removed;

4.2.10 ensure that there are adequate training resources for Super-users and end-users developed by suppliers or internally as required;

4.2.11 identify and take a lead for the super-user community across the systems, and ensure that they are trained and skilled to support end-users;

4.2.12 liaise with those responsible for the development of ERP systems across the NDA group and work jointly with them to agree developments which affect the functional scope above; and

4.2.13 ensure that supplier Service Continuity Plans are maintained up-to-date.

5. ROLE OF THE SUPPLIER FORUM

5.1 The Supplier Forum shall be accountable to the Commercial Systems Governance Board for oversight of the technology used in the Supplier Solution and interfacing third party solutions, ensuring that technological choices are made to maximise the long term value of the Supplier Solution as a business asset of the Authority.

5.2 The Supplier Forum shall consider:-

5.2.1 plans from the Authority for the development of standards, processes and organisational change which affect the systems, and information sharing about developments from the Government Commercial Function or wider policy matters;

5.2.2 feedback from the Authority on the operation of processes or interfaces shared across more than one system;

5.2.3 plans for the development of the Authority's IT infrastructure and systems as they are relevant to maintaining the interfaces between the Supplier Solution and third party solutions, on a confidential basis, for the purpose of ensuring that any impact on processes or interfaces shared across more than one system is understood and addressed; and

5.2.4 the development and delivery of joint action plans arising from the above.

6. CONTRACT MANAGEMENT MECHANISMS

6.1 Both Parties shall pro-actively manage risks attributed to them under the terms of this Agreement.

6.2 The Supplier shall develop, operate, maintain and amend, as agreed with the Authority, processes for:-

6.2.1 the identification and management of risks;

6.2.2 the identification and management of issues; and

6.2.3 monitoring and controlling project plans.

6.3 The Risk Register shall be updated by the Supplier and submitted for review at Service, System Management and Performance Review Meetings.

7. SERVICE, SYSTEM MANAGEMENT AND PERFORMANCE REVIEW MEETINGS

7.1 A monthly review meeting shall be held throughout the Term on a date to be agreed between the Parties.

7.2 The meetings shall be attended by the Account Manager of the Supplier and the *Contract Manager* of the Authority and any other persons considered necessary by the Authority or Supplier for the review.

7.3 The review meeting shall consider:

7.3.1 performance against the requirements of the contract including, but not limited to:-

(a) the Milestones as defined in Schedule 6.1 (*Implementation Plan*),

(b) Key Performance Indicators as defined in Schedule 2.2 (*Performance Levels*) and risk management; and

(c) any Service Credits payable by the Supplier to the Authority.

7.3.2 the overall operational performance of the System;

7.3.3 any risks, issues or concerns either of the Parties have with the System, relationship or Agreement.

7.4 The review of performance shall review Supplier performance for the previous Service Period and agree any Service Charges payable without prejudice to Schedule 7.1 (*Charges and Invoicing*).

APPENDIX 11

REPRESENTATION AND STRUCTURE OF FORMAL MEETINGS AND BOARDS

SERVICE, SYSTEM MANAGEMENT AND PERFORMANCE REVIEW MEETINGS

Meeting purpose	Review of Supplier Services delivery including Supplier System performance, delivery of Milestones, risks review and formal assessment of Key Performance Indicators
Authority attendees	Authority Project Victory Manager [Chairperson] Authority Commercial Systems, Data & Analytics Manager Authority Head of IT Transformation [by exception] and any other persons considered necessary by the Authority
Supplier attendees	Supplier *Account Manager* And any other persons considered necessary by the Supplier
Start date for Board meetings	From Effective Date as defined in Schedule 1 (Terms and Conditions)
Frequency of Board meetings	Monthly
Location of Board meetings	To be agreed between the Parties

JOINT IMPLEMENTATION BOARD

Board purpose	Review and assurance of interface design, build and test between the Supplier System and third party system(s) as specified by the Authority
Authority members of the Board	Authority Project Manager [Chairperson] Authority Commercial Systems, Data & Analytics Manager Authority Head of IT Transformation and any other persons considered necessary by the Authority
Supplier members of the Board	A maximum of two representatives from the Supplier who shall be empowered to make decisions on behalf of the Supplier
Third Party Supplier(s) of the Board	A maximum of two representatives from each third party supplier who shall be empowered to make decisions on behalf of each respective third party supplier
Start date for Board meetings	No sooner than Sept 2022
Frequency of Board meetings	Monthly or as required

Location of Board meetings	To be confirmed by the Authority prior to each Board

SUPPLIER FORUM (POST IMPLEMENTATION)

Forum purpose	Review and assurance of the performance of the system interfaces. The Forum will also discuss any forthcoming changes to either the Supplier System and/or third party system(s) that will affect the operation of the any system interface(s) to agree what, if any, development work is required to ensure the interface(s) remains operational
Authority members of the Forum	Authority Project Manager [Chairperson] Authority Commercial Systems, Data & Analytics Manager Authority Head of IT Transformation and any other persons considered necessary by the Authority
Supplier members of the Forum	A maximum of two representatives from the Supplier who shall be empowered to make decisions on behalf of the Supplier
Third Party Supplier(s) members of the Forum	A maximum of two representatives from each third party supplier who shall be empowered to make decisions on behalf of each respective third party supplier
Start date for Board meetings	No sooner than February 2023
Frequency of Board meetings	Quarterly or as required
Location of Board meetings	To be confirmed by the Authority prior to each Board

COMMERCIAL SYSTEMS GOVERNANCE BOARD

Authority Members of Project Victory Board	Authority Project Manager [Chairperson] Authority Commercial Systems, Data & Analytics Manager NDA Head of IT Transformation A representative from each of the Commercial teams across the NDA group businesses and any other persons considered necessary by the Authority
Start Date for Commercial Systems Governance Board meetings	No sooner than February 2023. Until this point, the Board shall be known as the Project Victory Board
Frequency of Commercial Systems Board meetings	Monthly to September February 2023 and then as agreed by the Authority
Location of Commercial Systems Board meetings	To be confirmed by the Authority prior to each Board

SCHEDULE 8.2

CHANGE CONTROL PROCEDURE

Issue No:	Summary of Change:
V0.1	Version for issue with ITT

I. **DEFINITIONS**

i. In this Schedule, the definitions set out in Schedule 1 shall apply.

8. **GENERAL PRINCIPLES OF CHANGE CONTROL PROCEDURE**

8.1 This Schedule sets out the procedure for dealing with Changes.

8.2 Operational Changes shall be processed in accordance with paragraph 15. If either Party is in doubt about whether a change falls within the definition of an Operational Change, then it must be processed as a Contract Change.

8.3 Document Change shall be processed in accordance with paragraph **Error! Reference source not found.**. If either Party is in doubt about whether a change falls within the definition of a Document Change, then it must be processed as a Contract Change.

8.4 The Parties shall deal with Contract Change as follows:-

8.4.1 either Party may request a Contract Change (and the Authority may raise a Contract Change on behalf of a Service Recipient) which they shall initiate by issuing a Change Request in accordance with paragraph 10;

8.4.2 unless this Agreement otherwise requires, the Supplier shall assess and document the potential impact of a proposed Contract Change in accordance with paragraph 11 before the Contract Change can be either approved or implemented;

8.4.3 the Authority shall have the right to request amendments to a Change Request, approve it or reject it in the manner set out in paragraph 12;

8.4.4 the Supplier shall have the right to reject a Change Request solely in the manner set out in paragraph 13;

8.4.5 save as otherwise provided in this Agreement, no proposed Contract Change shall be implemented by the Supplier until a Change Authorisation Note has been signed and issued by the Authority in accordance with paragraph 12.2; and

8.4.6 if a proposed Contract Change is a Fast-track Change, it shall be processed in accordance with paragraph 14.

8.5 To the extent that any Contract Change is a Project and/or otherwise requires testing and/or a programme for implementation, then the Parties shall document the requirements for any such testing and/or implementation, including the procedure to be followed, in the relevant Change Authorisation Note, and, where appropriate, the Change Authorisation Note relating to such a Contract Change shall specify:-

8.5.1 Milestones and/or a Key Milestone;

8.5.2 Milestone Date(s);

8.5.3 any Milestone Achievement Criteria; and

8.5.4 all information related to a Project (if relevant) as required pursuant to paragraph 11.1.8.

8.6 Until a Change Authorisation Note has been signed and issued by the Authority in accordance with paragraph 12.2, then:-

8.6.1 unless the Authority expressly agrees (or requires) otherwise in writing, the Supplier shall continue to supply the Services in accordance with the existing terms of this Agreement as if the proposed Contract Change did not apply; and

8.6.2 any discussions, negotiations or other communications which may take place between the Authority and the Supplier in connection with any proposed Contract Change, including the submission of any Change Communications, shall be without prejudice to each Party's other rights under this Agreement.

8.7 The Supplier shall:-

8.7.1 within ten (10) Working Days of the Authority's signature and issue of a Change Authorisation Note, deliver to the Authority a copy of this Agreement updated to reflect all Contract Changes agreed in the relevant Change Authorisation Note (including a copy of any documentation related to a Project (including the Project initiation document and Project plan (if applicable)) and annotated with a reference to the Change Authorisation Note pursuant to which the relevant Contract Changes were agreed; and

8.7.2 thereafter provide to the Authority such further copies of the updated Agreement as the Authority may from time to time request.

9. COSTS

9.1 Subject to paragraph **Error! Reference source not found.**:-

9.1.1 the costs of preparing each Change Request shall be borne by the Party making the Change Request; and

9.1.2 the costs incurred by the Supplier in undertaking an Impact Assessment shall be borne by the Party making the Change Request provided that the Authority shall not be required to pay any such costs if:-

(a) such costs are below £1000;

(b) the Supplier is able to undertake the Impact Assessment by using resources already deployed in the provision of the Services; or

(c) such costs exceed those in the accepted Impact Assessment Estimate.

9.2 The cost of any Contract Change shall be calculated and charged in accordance with the principles and day rates, product pricing, or development costs (as applicable) set out in Schedule 7.1 (*Charges and Invoicing*).

9.3 The Supplier shall:-

9.3.1 (provided that the Change is not a Non-Chargeable Change) only be entitled to add or increase the Charges in respect of the following Changes (with such Changes being "**Chargeable Changes**"):-

(a) a Project; and

(b) if it can demonstrate in the Impact Assessment that the proposed Contract Change requires additional resources and,

9.3.2 not be entitled to add to or increase the Charges in respect of the following (with such Changes being "**Non-Chargeable Changes**"):-

(a) any Change expressed in this Agreement as being a Non-Chargeable Change or at the Supplier's cost or expressly stated as not giving rise to any increase in the Charges;

(b) any Operational Change;

(c) any Document Change;

(d) a Change caused by a Change in Law in accordance with Clause 12.2 (Change in Law);

(e) implementation of a New Release, Update or Upgrade;

(f) any Change that secures efficiency savings (including by way of reduced running costs) to the extent such savings benefit the Supplier which over the Term meet or exceed the costs of implementing the Change;

(g) any Change required to remedy adverse audit findings due to a breach by the Supplier of its obligations under this Agreement;

(h) any Change caused by changes to the Supplier's own standard approaches, guidelines, methodologies or procedures;

(i) any Change caused by changes (not caused by other Chargeable Changes) to the Supplier Group; Supplier Personnel; Supplier Systems; or Sub-contractors or other resources used or required to be used by the Supplier to provide the Services in accordance with this Agreement;

(j) any Change in respect of which the costs and expenses associated with the Supplier complying with such Change are already included in the Charges; and

(k) any Change required as part of any error caused by the Supplier (or is Sub-contractors), any Defect, Default, Rectification Plan, or other Change required by the Supplier to enable the Supplier to comply with its obligations under this Agreement.

This paragraph 9.3.2 is not an exhaustive list of Changes in respect of which no additional or increased Charges shall apply.

10. CHANGE REQUEST

10.1 Either Party may issue a Change Request to the other Party at any time during the Term. A Change Request shall be substantially in the form of Appendix 12 and state whether the Party issuing the Change Request considers the proposed Contract Change to be a Fast-track Change.

10.2 If the Supplier issues the Change Request, then it shall also provide an Impact Assessment to the Authority as soon as is reasonably practicable but in any event within ten (10) Working Days of the date of issuing the Change Request.

10.3 If the Authority issues the Change Request, then the Supplier shall provide as soon as reasonably practical and in any event within ten (10) Working Days of the date of receiving the Change Request an estimate ("**Impact Assessment Estimate**") of the cost of preparing an Impact Assessment and the timetable for preparing it. The timetable shall provide for the completed Impact Assessment to

be received by the Authority within ten (10) Working Days of acceptance of the Impact Assessment Estimate or within any longer time period agreed by the Authority.

10.4 If the Authority accepts an Impact Assessment Estimate then following receipt of notice of such acceptance the Supplier shall provide the completed Impact Assessment to the Authority as soon as is reasonably practicable and in any event within the period agreed in the Impact Assessment Estimate. If the Supplier requires any clarification in relation to the Change Request before it can deliver the Impact Assessment, then it shall promptly make a request for clarification to the Authority and provided that sufficient information is received by the Authority to fully understand:-

10.4.1 the nature of the request for clarification; and

10.4.2 the reasonable justification for the request;

the time period to complete the Impact Assessment shall be extended by the time taken by the Authority to provide that clarification. The Authority shall respond to the request for clarification as soon as is reasonably practicable.

11. IMPACT ASSESSMENT

11.1 Each Impact Assessment shall be completed in good faith and shall include:-

11.1.1 details of the proposed Contract Change including the reason for the Contract Change; and

11.1.2 details of the impact of the proposed Contract Change on the Services and the Supplier's ability to meet its other obligations under this Agreement;

11.1.3 any variation to the terms of this Agreement that will be required as a result of that impact, including changes to:-

(a) the Services Description, the Performance Indicators and/or the Target Performance Levels;

(b) the format of Authority Data, as set out in the Services Description;

(c) the Milestones, Implementation Plan, any agreed Project and any other timetable previously agreed by the Parties;

(d) other services provided by third party contractors to the Authority, including any changes required by the proposed Contract Change to the Authority's IT infrastructure and / or the services or infrastructure provided by an Other Supplier;

11.1.4 details of the cost of implementing the proposed Contract Change (with application of the charging principles and pricing mechanisms set out in Schedule 7.1 (Charges and Invoicing) as appropriate);

11.1.5 details of the ongoing costs required by the proposed Contract Change when implemented, including any increase or decrease in the Charges, any alteration in the resources and/or expenditure required by either Party and any alteration to the working practices of either Party;

11.1.6 a timetable for the implementation, together with any proposals for the testing of the Contract Change;

11.1.7 details of how the proposed Contract Change will ensure compliance with any applicable Change in Law;

11.1.8 where the Contract Change is a Project:-

(a) a Project initiation document where requested by the Authority;

(b) a draft project plan that includes;-

(i) the proposed governance structure, including all relevant governance forums and/or boards for that Project;

(ii) the detail required pursuant to paragraph 11.1.6;

(iii) details on any interdependency between the Supplier and the Authority so as to enable the Authority to review the end-to-end plan for delivery, timeframes, sign-off and approvals; and

(iv) details on the expected benefits and outcomes of the Project;

(c) any minimum period of notice required to be given by the Authority in the event it wishes to cancel the proposed Project without cost, and any costs which are required to be paid by the Authority in accordance with this Agreement on cancellation earlier than such period of notice; and

(d) if the Project contemplates the licensing of third party Intellectual Property Rights, the licence and maintenance fees for such third party Intellectual Property Rights and information as to whether these fees may change during the course of the Project; and

11.1.9 such other information as the Authority may reasonably request in (or in response to) the Change Request.

11.2 Subject to the provisions of paragraph 11.3, the Authority shall review the Impact Assessment and respond to the Supplier in accordance with paragraph 12 within fifteen (15) Working Days of receiving the Impact Assessment.

11.3 If the Authority is the Receiving Party and the Authority reasonably considers that it requires further information regarding the proposed Contract Change so that it may properly evaluate the Change Request and the Impact Assessment, then within five (5) Working Days of receiving the Impact Assessment, it shall notify the Supplier of this fact and detail the further information that it requires. The Supplier shall then re-issue the relevant Impact Assessment to the Authority within ten (10) Working Days of receiving such notification. At the Authority's discretion, the Parties may repeat the process described in this paragraph 11.3 until the Authority is satisfied that it has sufficient information to properly evaluate the Change Request and Impact Assessment.

11.4 The calculation of costs for the purposes of paragraphs 11.1.4 and 11.1.5 shall:-

11.4.1 facilitate the Financial Transparency Objectives;

11.4.2 include estimated volumes of each type of resource to be employed and the applicable rate card (including application of the Rate Card and/or Development Charges as set out in Schedule 7.1 (Charges and Invoicing));

11.4.3 include full disclosure of any assumptions underlying such Impact Assessment;

11.4.4 include evidence of the cost of any assets required for the Change; and

11.4.5 include details of any new Sub-contracts necessary to accomplish the Change.

12. AUTHORITY'S RIGHT OF APPROVAL

12.1 Within twenty (20) Working Days of receiving the Impact Assessment from the Supplier or within ten (10) Working Days of receiving the further information that it may request pursuant to

paragraph 11.3, the Authority shall evaluate the Change Request and the Impact Assessment and shall do one of the following:-

12.1.1 approve the proposed Contract Change at the Commercial Systems Governance Board, in which case the Parties shall follow the procedure set out in paragraph 12.2;

12.1.2 in its absolute discretion reject the Contract Change at the Commercial Systems Governance Board, in which case it shall notify the Supplier of the rejection. The Authority shall not reject any proposed Contract Change to the extent that the Contract Change is necessary for the Supplier or the Services to comply with any Changes in Law. If the Authority does reject a Contract Change, then it shall explain its reasons in writing to the Supplier as soon as is reasonably practicable following such rejection; or

12.1.3 in the event that it reasonably believes that a Change Request or Impact Assessment contains errors or omissions, require the Supplier to modify the relevant document accordingly, in which event the Supplier shall make such modifications within five (5) Working Days of such request. Subject to paragraph 11.3, on receiving the modified Change Request and/or Impact Assessment, the Authority shall approve or reject the proposed Contract Change within ten (10) Working Days.

12.2 If the Authority approves the proposed Contract Change pursuant to paragraph 12.1 and it has not been rejected by the Supplier in accordance with paragraph 13, then it shall inform the Supplier and the Supplier shall prepare two (2) copies of a Change Authorisation Note which it shall sign and deliver to the Authority for its signature. Following receipt by the Authority of the Change Authorisation Note, it shall sign both copies and return one copy to the Supplier. On the Authority's signature the Change Authorisation Note shall constitute (or, where the Authority has agreed to or required the implementation of a Change prior to signature of a Change Authorisation Note, shall constitute confirmation of) a binding variation to this Agreement.

12.3 If the Authority does not sign the Change Authorisation Note within ten (10) Working Days, then the Supplier shall have the right to notify the Authority and if the Authority does not sign the Change Authorisation Note within five (5) Working Days of such notification, then the Supplier may refer the matter to the Expedited Dispute Timetable pursuant to the Dispute Resolution Procedure.

13. SUPPLIER'S RIGHT OF APPROVAL

Following an Impact Assessment, if:-

13.1 the Supplier reasonably believes that any proposed Contract Change which is requested by the Authority would:-

13.1.1 materially and adversely affect the risks to the health and safety of any person; and/or

13.1.2 require the Services to be performed in a way that infringes any Law; and/or

13.2 the Supplier demonstrates to the Authority's reasonable satisfaction that the proposed Contract Change is technically impossible to implement and neither the Supplier Solution nor the Services Description state that the Supplier does have the technical capacity and flexibility required to implement the proposed Contract Change,

then the Supplier shall be entitled to reject the proposed Contract Change and shall notify the Authority in writing of its reasons for doing so within five (5) Working Days after the date on which it is obliged to deliver the Impact Assessment pursuant to paragraph 10.3.

14. FAST-TRACK CHANGES

14.1 The Parties acknowledge that to ensure operational efficiency there may be circumstances where it is desirable to expedite the processes set out above.

14.2 The Party requesting a Contract Change shall notify the other Party in accordance with paragraph 10.1 when the Contract Change is a Fast-track Change. The Parties shall use the process set out in paragraphs 10, 11, 12 and 13 but with reduced timescales and such reduced timescales shall be agreed between the Parties in writing.

15. OPERATIONAL CHANGE PROCEDURE

15.1 Any Operational Changes identified by the Supplier to improve operational efficiency of the Services may be implemented by the Supplier without following the Change Control Procedure for proposed Contract Changes provided they do not:-

15.1.1 have an impact on the business of the Authority;

15.1.2 adversely affect the interfaces or interoperability of the Services with any of the Authority's IT infrastructure or the services or infrastructure of an Other Supplier;

15.1.3 require a change to this Agreement;

15.1.4 have a direct impact on use of the Services; or

15.1.5 involve the Authority in paying any additional Charges or other costs.

15.2 The Authority may request an Operational Change by submitting a written request for Operational Change ("**RFOC**") to the Supplier Representative.

15.3 The RFOC shall include the following details:-

15.3.1 the proposed Operational Change; and

15.3.2 the time-scale for completion of the Operational Change.

15.4 The Supplier shall inform the Authority of any impact on the Services that may arise from the proposed Operational Change.

15.5 The Supplier shall complete the Operational Change by the agreed upon timescale specified for completion of the Operational Change in the RFOC, and shall promptly notify the Authority when the Operational Change is completed.

15.6 The Authority may, at its discretion, make basic Operational Changes itself, such as changes to field names (or additions) and creating or removing users.

16. DOCUMENT CHANGE PROCEDURE

16.1 The Parties shall maintain the List of Controlled Documents which shall set out the names and version numbers of the Controlled Documents existing from time to time during the Term. A preliminary version of the List of Controlled Documents as at the Effective Date is set out in Appendix 14 and the Parties shall update this document during Implementation in accordance with the procedure set out in paragraph 16.2.

16.2 Controlled Documents shall only be effective when approved in writing by the authorised representative of each Party and, unless and until so approved and given an appropriate version number, shall constitute draft documents only.

16.3 Upon:

16.3.1 a new version of a Controlled Document being approved (in accordance with paragraph 16.2) and the version number being incremented;

16.3.2 a new Controlled Document being approved, where the Parties have agreed to create a new Controlled Document; and

16.3.3 the Parties agreeing that an existing Controlled Document should no longer be classified as a Controlled Document,

the Supplier shall update the information in the List of Controlled Documents accordingly.

16.4 Where any proposed change to a Controlled Document would, if approved, create an inconsistency with any other provisions within this Agreement or would require a Change to another part of the Agreement such proposed change shall not be effective (even if approved within the Controlled Document) unless and until the Parties have also approved an associated change to the relevant part of the Agreement using the Change Control Procedure applicable for a Contract Change.

17. COMMUNICATIONS

For any Change Communication to be valid under this Schedule, it must be sent to either the Authority Change Manager or the Supplier Change Manager, as applicable. The provisions of Clause 4.1 shall apply to a Change Communication as if it were a notice.

APPENDIX 12

CHANGE REQUEST FORM

CR NO.:	TITLE:	TYPE OF CHANGE:
CONTRACT:	REQUIRED BY DATE:	
ACTION:	NAME:	DATE:
RAISED BY:		
AREA(S) IMPACTED (*OPTIONAL FIELD*):		
ASSIGNED FOR IMPACT ASSESSMENT BY:		
ASSIGNED FOR IMPACT ASSESSMENT TO:		
SUPPLIER REFERENCE NO.:		
FULL DESCRIPTION OF REQUESTED CONTRACT CHANGE (INCLUDING PROPOSED CHANGES TO THE WORDING OF THE CONTRACT):		
DETAILS OF ANY PROPOSED ALTERNATIVE SCENARIOS:		
REASONS FOR AND BENEFITS AND DISADVANTAGES OF REQUESTED CONTRACT CHANGE		
SIGNATURE OF REQUESTING CHANGE OWNER:		
DATE OF REQUEST:		

APPENDIX 13

CHANGE AUTHORISATION NOTE

CR NO.:	TITLE:	TYPE OF CHANGE:
CONTRACT:	REQUIRED BY DATE:	
ACTION:	NAME:	DATE:
[KEY MILESTONE DATE: [if any]]		
DETAILED DESCRIPTION OF CONTRACT CHANGE FOR WHICH IMPACT ASSESSMENT IS BEING PREPARED AND WORDING OF RELATED CHANGES TO THE CONTRACT:		
[DETAILED DESCRIPTION OF ANY PROJECT [if any] INCLUDING A PROJECT INITIATION DOCUMENT, PROJECT PLAN AND OTHER INFORMATION REQUIRED IN ACCORDANCE WITH PARAGRAPH 8.5 OF SCHEDULE 8.2 (CONTRACT CHANGE PROCEDURE)		
PROPOSED ADJUSTMENT TO THE CHARGES RESULTING FROM THE CONTRACT CHANGE:		
DETAILS OF PROPOSED ONE-OFF ADDITIONAL CHARGES AND MEANS FOR DETERMINING THESE (E.G. FIXED PRICE BASIS):		

SIGNED ON BEHALF OF THE AUTHORITY:		SIGNED ON BEHALF OF THE SUPPLIER:	
Signature:	……	Signature:	……
Name:	……	Name:	……
Position:	……	Position:	……
Date:	……	Date:	……

APPENDIX 14

LIST OF CONTROLLED DOCUMENTS AS AT THE EFFECTIVE DATE

Controlled Document	Cited	Version Number

SCHEDULE 8.3

DISPUTE RESOLUTION PROCEDURE

Issue No:	Summary of Change:
V0.1	Version for issue with ITT

18. **DEFINITIONS**

18.1 In this Schedule, the definitions set out in Schedule 1 shall apply.

19. **DISPUTE NOTICES**

19.1 If a Dispute arises then:-

19.1.1 the Authority Representative and the Supplier Representative shall attempt in good faith to resolve the Dispute; and

19.1.2 if such attempts are not successful within a reasonable period, not being longer than twenty (20) Working Days, either Party may issue to the other a Dispute Notice.

19.2 A Dispute Notice:-

19.2.1 shall set out:-

(a) the material particulars of the Dispute;

(b) the reasons why the Party serving the Dispute Notice believes that the Dispute has arisen; and

(c) if the Party serving the Dispute Notice believes that the Dispute should be dealt with under the Expedited Dispute Timetable, the reason why; and

19.2.2 may specify in accordance with the requirements of paragraphs 26.2 and 26.3 that the Party issuing the Dispute Notice has determined (in the case of the Authority) or considers (in the case of the Supplier) that the Dispute is a Multi-Party Dispute, in which case paragraph 19.3 shall apply.

19.3 If a Dispute Notice specifies that the Dispute has been determined or is considered to be a Multi-Party Dispute pursuant to paragraph 19.2.2, then:-

19.3.1 if it is served by the Authority it shall be treated as a Multi-Party Procedure Initiation Notice; and

19.3.2 if it is served by the Supplier it shall be treated as a Supplier Request, and in each case the provisions of paragraph 26 shall apply.

19.4 Subject to paragraphs 19.5 and 20.2 and so long as the Authority has not served a Multi-Party Procedure Initiation Notice in respect of the relevant Dispute, following the issue of a Dispute Notice the Parties shall seek to resolve the Dispute:-

19.4.1 first by commercial negotiation (as prescribed in paragraph 21);

19.4.2 then, if either Party serves a Mediation Notice, by mediation (as prescribed in paragraph 22); and

19.4.3 lastly by recourse to litigation (in accordance with Clause 42 (*Governing Law and Jurisdiction)*).

19.5 Specific issues shall be referred to Expert Determination (as prescribed in paragraph 23) where specified under the provisions of this Agreement and may also be referred to Expert Determination where otherwise appropriate as specified in paragraph 23.1.

19.6 Unless agreed otherwise in writing, the Parties shall continue to comply with their respective obligations under this Agreement regardless of the nature of the Dispute and notwithstanding any issue of a Dispute Notice or a Multi-Party Procedure Initiation Notice or proceedings under paragraph 9.

20. EXPEDITED DISPUTE TIMETABLE

20.1 In exceptional circumstances where the use of the times in this Schedule would be unreasonable, including, by way of example, where one Party would be materially disadvantaged by a delay in resolving the Dispute, the Parties may agree to use the Expedited Dispute Timetable. If the Parties are unable to reach agreement on whether to use the Expedited Dispute Timetable within five (5) Working Days of the issue of a Dispute Notice, the use of the Expedited Dispute Timetable shall be at the sole discretion of the Authority.

20.2 If the Expedited Dispute Timetable is to be used pursuant to the provisions of paragraph 20.1 or is otherwise specified under the provisions of this Agreement, then the following periods of time shall apply in lieu of the time periods specified in the applicable paragraphs:-

20.2.1 in paragraph 21.2.3), ten (10) Working Days;

20.2.2 in paragraph 22.2, ten (10) Working Days; and

20.2.3 in paragraph 23.2, five (5) Working Days.

20.3 If at any point it becomes clear that an applicable deadline cannot be met or has passed, the Parties may (but shall be under no obligation to) agree in writing to extend the deadline. If the Parties fail to agree within two (2) Working Days after the deadline has passed, the Authority may set a revised deadline provided that it is no less than five (5) Working Days before the end of the period of time specified in the applicable paragraphs (or two (2) Working Days in the case of paragraph 23.2). Any agreed extension shall have the effect of delaying the start of the subsequent stages by the period agreed in the extension. If the Authority fails to set such a revised deadline then the use of the Expedited Dispute Timetable shall cease and the normal time periods shall apply from that point onwards.

21. COMMERCIAL NEGOTIATION

21.1 Following the service of a Dispute Notice, then, so long as the Authority has not served a Multi-Party Procedure Initiation Notice in respect of the relevant Dispute, the Authority and the Supplier shall make reasonable endeavours to resolve the Dispute as soon as possible by commercial negotiation between the Authority's Group Commercial Director and the Supplier's Managing Director.

21.2 If:-

21.2.1 either Party is of the reasonable opinion that the resolution of a Dispute by commercial negotiation, or the continuance of commercial negotiation, will not result in an appropriate solution;

21.2.2 the Parties have already held discussions of a nature and intent (or otherwise were conducted in the spirit) that would equate to the conduct of commercial negotiation in accordance with this paragraph 21; or

21.2.3 the Parties have not settled the Dispute in accordance with paragraph 21.1 within thirty (30) Working Days of service of the Dispute Notice,

either Party may serve a written notice to proceed to mediation in accordance with paragraph 22 (a "**Mediation Notice**").

22. MEDIATION

22.1 If a Mediation Notice is served, the Parties shall attempt to resolve the dispute in accordance with the version of CEDR's Model Mediation Procedure which is current at the time the Mediation Notice is served (or such other version as the Parties may agree).

22.2 If the Parties are unable to agree on the joint appointment of an independent person to mediate the Dispute within twenty (20) Working Days from (and including) the service of a Mediation Notice then either Party may apply to CEDR to nominate such a person.

22.3 If the Parties are unable to reach a settlement in the negotiations at the mediation, and only if both Parties so request and the Mediator agrees, the Mediator shall produce for the Parties a non-binding recommendation on terms of settlement. This shall not attempt to anticipate what a court might order but shall set out what the Mediator suggests are appropriate settlement terms in all of the circumstances.

22.4 Any settlement reached in the mediation shall not be legally binding until it has been reduced to writing and signed by, or on behalf of, the Parties (in accordance with the Change Control Procedure where appropriate). The Mediator shall assist the Parties in recording the outcome of the mediation.

23. EXPERT DETERMINATION

23.1 If a Dispute relates to any:

23.1.1 aspect of the technology underlying the provision of the Services or otherwise relates to a technical matter of an IT nature; or

23.1.2 accounting or financing matters,

and the Dispute has not been resolved by commercial negotiation in accordance with paragraph 21 or, if applicable, mediation in accordance with paragraph 22, then either Party may by written notice to the other request (agreement to which request shall not be unreasonably withheld or delayed) that the Dispute be referred to an Expert for determination.

23.2 The Expert shall be appointed by agreement in writing between the Parties, but in the event of a failure to agree within ten (10) Working Days of the relevant request made pursuant to paragraph 23.1, or if the person appointed is unable or unwilling to act, the Expert shall be appointed:-

23.2.1 if the Dispute relates to any aspect of the technology underlying the provision of the Services or a matter of an IT technical nature, on the instructions of the [President of the British Computer Society] (or any other association that has replaced the British Computer Society);

23.2.2 if the Dispute relates to a matter of an accounting or financial technical nature, on the instructions of the [President of the Institute of Chartered Accountants of England and Wales]; or

23.2.3 if the Dispute relates to a matter of a technical nature not falling within paragraphs 23.2.1 or 23.2.2, on the instructions of the president (or equivalent) of:-

(a) an appropriate body agreed between the Parties; or

(b) if the Parties do not reach agreement on the relevant body within fifteen (15) Working Days of the relevant request made pursuant to paragraph 23.1, such body as may be specified by the [President of the Law Society] on application by either Party.

23.3 The Expert shall act on the following basis:-

23.3.1 he/she shall act as an expert and not as an arbitrator and shall act fairly and impartially;

23.3.2 the Expert's determination shall (in the absence of a material failure to follow the agreed procedures) be final and binding on the Parties;

23.3.3 the Expert shall decide the procedure to be followed in the determination and shall be requested to make his/her determination within thirty (30) Working Days of his appointment or as soon as reasonably practicable thereafter and the Parties shall assist and provide the documentation that the Expert requires for the purpose of the determination;

23.3.4 any amount payable by one Party to another as a result of the Expert's determination shall be due and payable within twenty (20) Working Days of the Expert's determination being notified to the Parties;

23.3.5 the process shall be conducted in private and shall be confidential; and

23.3.6 the Expert shall determine how and by whom the costs of the determination, including his/her fees and expenses, are to be paid.

24. **[NOT USED]**

25. **URGENT RELIEF**

Either Party may at any time take proceedings or seek remedies before any court or tribunal of competent jurisdiction:-

25.1 for interim or interlocutory remedies in relation to this Agreement or infringement by the other Party of that Party's Intellectual Property Rights; and/or

25.2 where compliance with paragraph 19.1 and/or referring the Dispute to mediation may leave insufficient time for that Party to commence proceedings before the expiry of the limitation period.

26. **MULTI-PARTY DISPUTES**

26.1 All Multi--Party Disputes shall be resolved in accordance with the procedure set out in this paragraph 26 (the "**Multi--Party Dispute Resolution Procedure**").

26.2 If at any time following the issue of a Dispute Notice, the Authority reasonably considers that the matters giving rise to the Dispute involve one or more Related Third Parties, then the Authority shall be entitled to determine that the Dispute is a Multi--Party Dispute and to serve a notice on the Supplier which sets out the Authority's determination that the Dispute is a Multi--Party Dispute and specifies the Related Third Parties which are to be involved in the Multi--Party Dispute Resolution Procedure, such notice a "**Multi--Party Procedure Initiation Notice**".

26.3 If following the issue of a Dispute Notice but before the Dispute has been referred to Expert Determination, the Supplier has reasonable grounds to believe that the matters giving rise to the Dispute have been contributed to by one or more Related Third Parties, the Supplier may serve a Supplier Request on the Authority.

26.4 The Authority shall (acting reasonably) consider each Supplier Request and shall determine within five (5) Working Days whether the Dispute is:-

26.4.1 a Multi--Party Dispute, in which case the Authority shall serve a Multi--Party Procedure Initiation Notice on the Supplier; or

26.4.2 not a Multi--Party Dispute, in which case the Authority shall serve written notice of such determination upon the Supplier and the Dispute shall be treated in accordance with paragraphs 20 to 25.

26.5 If the Authority has determined, following a Supplier Request, that a Dispute is not a Multi--Party Dispute, the Supplier may not serve another Supplier Request with reference to the same Dispute.

26.6 Following service of a Multi--Party Procedure Initiation Notice a Multi--Party Dispute shall be dealt with by a board (in relation to such Multi--Party Dispute, the "**Multi--Party Dispute Resolution Board**") comprising representatives from the following parties to the Multi--Party Dispute, each of whom shall be of a suitable level of seniority to finalise any agreement with the other parties to settle the Multi--Party Dispute:-

26.6.1 the Authority;

26.6.2 the Supplier;

26.6.3 each Related Third Party involved in the Multi-Party Dispute;

26.6.4 (to the extent different from paragraph 9.6.3 above) any Service Recipient affected by the Multi-Party Dispute; and

26.6.5 any other representatives of any of the Parties, any Related Third Parties or Service Recipients whom the Authority considers necessary,

(together "**Multi--Party Dispute Representatives**").

26.7 The Parties agree that the Multi--Party Dispute Resolution Board shall seek to resolve the relevant Multi--Party Dispute in accordance with the following principles and procedures:-

26.7.1 the Parties shall procure that their Multi--Party Dispute Representatives attend, and shall use their best endeavours to procure that the Multi--Party Dispute Representatives of each Related Third Party attend, all meetings of the Multi--Party Dispute Resolution Board in respect of the Multi--Party Dispute;

26.7.2 the Multi--Party Dispute Resolution Board shall first meet within ten (10) Working Days of service of the relevant Multi--Party Procedure Initiation Notice at such time and place as the Parties may agree or, if the Parties do not reach agreement on the time and place within five (5) Working Days of service of the relevant Multi--Party Procedure Initiation Notice, at the time and place specified by the Authority, provided such place is at a neutral location within England and that the meeting is to take place between 9.00am and 5.00pm on a Working Day; and

26.7.3 in seeking to resolve or settle any Multi--Party Dispute, the members of the Multi--Party Dispute Resolution Board shall have regard to the principle that a Multi--Party Dispute should be determined based on the contractual rights and obligations between the Parties and the Related Third Parties and that any apportionment of costs should reflect the separate components of the Multi--Party Dispute.

26.8 If a Multi--Party Dispute is not resolved between the Parties and all Related Third Parties within twenty-five (25) Working Days of the issue of the Multi--Party Procedure Initiation Notice (or such longer period as the Parties may agree in writing), then:-

26.8.1 either Party may serve a Mediation Notice in respect of the Multi--Party Dispute in which case paragraph 22 shall apply; and/or

26.8.2 either Party may request that the Multi--Party Dispute is referred to an Expert in which case paragraph 23 shall apply,

and in each case references to the "**Supplier**" or the "**Parties**" in such provisions shall include a reference to all Related Third Parties.

SCHEDULE 8.4

REPORTS AND RECORDS PROVISIONS

Issue No:	Summary of Change:
V0.1	Version for issue with ITT

I. DEFINITIONS

i. In this Schedule, the definitions set out in Schedule 1 shall apply.-

27. REPORTS

The Authority may require any or all of the following reports:-

27.1 delay reports;

27.2 reports relating to Testing and tests carried out under Schedule 2.4 (*Security Management*) and Schedule 8.6 (*Service Continuity Plan and Corporate Resolution Planning*);

27.3 reports which the Supplier is required to supply as part of the Management Information;

27.4 annual reports on the Insurances;

27.5 security reports; and

27.6 Force Majeure Event reports.

28. RECORDS

28.1 The Supplier shall retain and maintain all the records (including superseded records) referred to in paragraph **Error! Reference source not found.** and Appendix 15 (together "**Records**"):-

28.1.1 in accordance with the requirements of The National Archives and Good Industry Practice;

28.1.2 in chronological order;

28.1.3 in a form that is capable of audit; and

28.1.4 at its own expense.

28.2 The Supplier shall make the Records available for inspection to the Authority on request, subject to the Authority giving reasonable notice as per Schedule 7.5 section 3.4

28.3 Where Records are retained in electronic form, the original metadata shall be preserved together with all subsequent metadata in a format reasonably accessible to the Authority.

28.4 The Supplier shall, during the Term and for a period of at least seven (7) years following the expiry or termination of this Agreement, maintain or cause to be maintained complete and accurate documents and records in relation to the provision of the Services including but not limited to all Records.

28.5 Records that contain financial information shall be retained and maintained in safe storage by the Supplier for a period of at least seven (7) years after the expiry or termination of this Agreement.

28.6 Without prejudice to the foregoing, the Supplier shall provide the Authority:-

28.6.1 as soon as they are available, and in any event within sixty (60) Working Days after the end of the first six (6) months of each financial year of the Supplier during the Term, a copy, certified as a true copy by an authorised representative of the Supplier, of its un-audited interim accounts.

APPENDIX 15

TRANSPARENCY REPORTS – [NOT USED]

APPENDIX 16

RECORDS TO BE KEPT BY THE SUPPLIER

The records to be kept by the Supplier are:-

29. this Agreement, its Schedules and all amendments to such documents;

30. all other documents which this Agreement expressly requires to be prepared;

31. documents prepared by the Supplier in support of Performance Levels;

32. records relating to the appointment and succession of the Supplier Representative and each member of the Key Personnel;

33. notices, reports and other documentation submitted by any Expert;

34. all operation and maintenance manuals prepared by the Supplier for the purpose of maintaining the provision of the Services and the underlying IT Environment and Supplier Equipment;

35. documents prepared by the Supplier or received by the Supplier from a third party relating to a Force Majeure Event;

36. all formal notices, reports or submissions made by the Supplier to the Authority Representative in connection with the provision of the Services;

37. all certificates, licences, registrations or warranties in each case obtained by the Supplier in relation to the provision of the Services;

38. documents prepared by the Supplier in support of claims for the Charges;

39. documents submitted by the Supplier pursuant to the Change Control Procedure;

40. documents submitted by the Supplier pursuant to invocation by it or the Authority of the Dispute Resolution Procedure;

41. documents evidencing any change in ownership or any interest in any or all of the shares in the Supplier and/or the Guarantor, where such change may cause a change of Control; and including documents detailing the identity of the persons changing such ownership or interest;

42. invoices and records related to VAT sought to be recovered by the Supplier;

43. financial records, including audited and un-audited accounts of the Guarantor and the Supplier;

44. records required to be retained by the Supplier by Law, including in relation to health and safety matters and health and safety files and all consents;

45. all documents relating to the insurances to be maintained under this Agreement and any claims made in respect of them;

46. all journals and audit trail data referred to in Schedule 2.4 (*Security Management Plan*); and

47. all other records, notices or certificates required to be produced and/or maintained by the Supplier pursuant to this Agreement.

SCHEDULE 8.5

EXIT MANAGEMENT

Issue No:	Summary of Change:
V0.1	Version for issue with ITT

I. DEFINITIONS

i. In this Schedule, the definitions set out in Schedule 1 (*Definitions)* shall apply.

48. OBLIGATIONS DURING THE TERM TO FACILITATE EXIT

48.1 During the Term, the Supplier shall:-

48.1.1 Within three months of the Effective Date, create and then subsequently maintain a register of all:-

(a) Assets, detailing their:-

(i) make, model and asset number;

(ii) ownership and status as either Exclusive Assets or Non-Exclusive Assets;

(iii) Net Book Value;

(iv) condition and physical location; and

(v) use (including technical specifications);

(b) Sub-contracts and other relevant agreements (including relevant software licences, maintenance and support agreements and equipment rental and lease agreements) required for the performance of the Services;

48.1.2 agree the format of the Register with the Authority as part of the process of agreeing the Exit Plan; and

48.1.3 at all times keep the Register up to date, in particular in the event that Assets, Sub-contracts or other relevant agreements are added to or removed from the Services.

48.2 The Supplier shall ensure that all Exclusive Assets listed in the Register are clearly marked to identify that they are exclusively used for the provision of the Services under this Agreement.

48.3 Each Party shall appoint a person for the purposes of managing the Parties' respective obligations under this Schedule and provide written notification of such appointment to the other Party within three (3) months of the Effective Date. The Supplier's Exit Manager shall be responsible for maintaining the Exit Plan and ensuring that the Supplier and its employees, agents and Sub-contractors comply with this Schedule. The Supplier shall ensure that its Exit Manager has the requisite authority to arrange and procure any resources of the Supplier as are reasonably necessary to enable the Supplier to comply with the requirements set out in this Schedule. The Parties' Exit Managers will liaise with one another in relation to all issues relevant to the termination of this Agreement and all matters connected with this Schedule and each Party's compliance with it.

49. OBLIGATIONS TO ASSIST ON RE-TENDERING OF SERVICES

49.1 On reasonable notice at any point during the Term, the Supplier shall provide to the Authority and/or its potential Replacement Suppliers (subject to the potential Replacement Suppliers entering into reasonable written confidentiality undertakings), the following material and information in order to facilitate the preparation by the Authority of any invitation to tender and/or to facilitate any potential Replacement Suppliers undertaking due diligence:-

49.1.1 an inventory of Authority Data in the Supplier's possession or control;

49.2 The Supplier acknowledges that the Authority may disclose the Supplier's Confidential Information to any Service Recipient,

49.3 The Supplier shall:-

49.3.1 notify the Authority within five (5) Working Days of any material change to the Exit Information which may adversely impact upon the potential transfer and/or continuance of the provision of any Services and shall consult with the Authority regarding such proposed material changes; and

49.3.2 provide complete updates of the Exit Information on an as--requested basis as soon as reasonably practicable and in any event within ten (10) Working Days of a request in writing from the Authority.

49.4 The Supplier may charge the Authority for its reasonable additional costs to the extent the Authority requests more than four (4) updates in any six (6) month period.

49.5 The Exit Information shall be accurate and complete in all material respects and the level of detail to be provided by the Supplier shall be such as would be reasonably necessary to enable a third party to:-

49.5.1 prepare an informed offer for those Services; and

49.5.2 not be disadvantaged in any subsequent procurement process compared to the Supplier (if the Supplier is invited to participate).

50. EXIT PLAN

50.1 The Supplier shall, within three (3) months after the Effective Date, deliver to the Authority an Exit Plan which:-

50.1.1 sets out the Supplier's proposed methodology for delivering Authority data;

50.2 The Parties shall use reasonable endeavours to agree the contents of the Exit Plan. If the Parties are unable to agree the contents of the Exit Plan within twenty (20) Working Days of its submission, then such Dispute shall be resolved in accordance with the Dispute Resolution Procedure.

50.3 The Exit Plan shall set out, as a minimum:-

50.3.1 how the Exit Information is obtained;

50.3.2 separate mechanisms for dealing with Ordinary Exit and Emergency Exit, the provisions relating to Emergency Exit being prepared on the assumption that the Supplier may be unable to provide the full level of assistance which is required by the provisions relating to Ordinary Exit and in the case of Emergency Exit, provision for the supply by the Supplier of all such reasonable assistance as the Authority shall require to enable the Authority or its sub-contractors to provide the Services;

50.3.3 any other element that the Authority reasonably requires to be addressed.

Finalisation of the Exit Plan

50.4 Within twenty (20) Working Days after service of a Termination Notice by either Party or six (6) months prior to the expiry of this Agreement, the Supplier will submit for the Authority's approval the Exit Plan in a final form that could be implemented immediately. The final form of the Exit Plan shall be prepared on a basis consistent with the principles set out in this Schedule and shall reflect any changes in the provision of the Services that have occurred since the Exit Plan was last agreed.

50.5 The Parties will meet and use their respective reasonable endeavours to agree the contents of the final form of the Exit Plan and the Supplier shall incorporate additional detail as the Authority deems

necessary. If the Parties are unable to agree the contents of the Exit Plan within twenty (20) Working Days following its delivery to the Authority then such Dispute shall be resolved in accordance with the Dispute Resolution Procedure. Until the agreement of the final form of the Exit Plan, the Supplier shall provide the Termination Services in accordance with the principles set out in this Schedule and the last approved version of the Exit Plan (insofar as relevant).

51. TERMINATION SERVICES

Notification of Requirements for Termination Services

51.1 The Authority shall be entitled to require the provision of Termination Services at any time during the Term by giving written notice to the Supplier (a "**Termination Assistance Notice**") at least four (4) months prior to the date of Partial Termination, termination or expiry of this Agreement or as soon as reasonably practicable (but in any event, not later than one (1) month) following the service by either Party of a Termination Notice. The Termination Assistance Notice shall specify:-

51.1.1 the date from which Termination Services are required;

51.1.2 the nature of the Termination Services required; and

51.1.3 the period during which it is anticipated that Termination Services will be required, which shall continue no longer than twenty four (24) months after the date that the Supplier ceases to provide the relevant terminated Services.

51.2 The Authority shall have:-

51.2.1 an option to extend the period of assistance beyond the period specified in the relevant Termination Assistance Notice provided that such extension shall not extend for more than six (6) months after the date the Supplier ceases to provide the terminated Services or, if applicable, beyond the end of the Termination Assistance Period and provided that it shall notify the Supplier to such effect no later than twenty (20) Working Days prior to the date on which the provision of Termination Services is otherwise due to expire; and

51.2.2 the right to terminate its requirement for Termination Services by serving not less than twenty (20) Working Days' written notice upon the Supplier to such effect.

Termination Assistance Period

51.3 Throughout the Termination Assistance Period, or such shorter period as the Authority may require, the Supplier shall:-

51.3.1 continue to provide the Services (as applicable) and, if required by the Authority pursuant to paragraph 2.1, provide the Termination Services;

51.3.2 co-operate with the Service Recipients and any Replacement Supplier;

51.3.3 in addition to providing the Services and the Termination Services, provide to the Authority any reasonable assistance requested by the Authority to allow the provision of the Services to continue without interruption following the Partial Termination, termination or expiry of this Agreement and to facilitate the orderly transfer of responsibility for and conduct of the provision of the Services to the Authority, any Service Recipient and/or its Replacement Supplier;

51.3.4 use all reasonable endeavours to reallocate resources to provide such assistance as is referred to in paragraph 3 without additional costs to the Authority;

51.3.5 provide the Services and the Termination Services at no detriment to the Target Performance Levels, and continue to participate in the governance arrangements under Schedule 8.1 *(Governance)*, save to the extent that the Parties agree otherwise in accordance with paragraph 5; and

51.3.6 at the Authority's request and on reasonable notice, deliver up--to--date Registers to the Authority.

51.4 Without prejudice to the Supplier's obligations under paragraph 2.3, if it is not possible for the Supplier to reallocate resources to provide such assistance as is referred to in paragraph 3 without additional costs to the Authority, any additional costs incurred by the Supplier in providing such reasonable assistance which is not already in the scope of the Termination Services or the Exit Plan shall be subject to the Change Control Procedure.

51.5 If the Supplier demonstrates to the Authority's reasonable satisfaction that transition of the provision of the Services and provision of the Termination Services during the Termination Assistance Period will have a material, unavoidable adverse effect on the Supplier's ability to meet one or more particular Target Performance Level(s), the Parties shall vary the relevant Target Performance Level(s) and/or the applicable Service Credits to take account of such adverse effect.

Termination Obligations

51.6 The Supplier shall comply with all of its obligations contained in the Exit Plan in respect of any Partial Termination or termination or expiry of this Agreement.

51.7 At the end of the Termination Assistance Period (or earlier if this does not adversely affect the Supplier's performance and/or delivery of the Services and the Termination Services and its compliance with the other provisions of this Schedule) in respect of the Services that have been terminated, the Supplier shall:-

51.7.1 cease to use the Authority Data;

51.7.2 comply with any directions given by the Authority relating to the Authority Data;

51.7.3 provide the Authority and/or the Replacement Supplier with a complete and uncorrupted version of the Authority Data in a standard electronic form (supported by the Supplier;

51.7.4 erase from any computers, storage devices and storage media that are to be retained by the Supplier after the end of the Termination Assistance Period all Authority Data and promptly certify to the Authority that it has completed such deletion;

51.7.5 All data that is in systematic archival rotation will be erased as per the Suppliers system archival rotation.

51.7.6 securely destroy or confidentially dispose of any information or documentation to which it is not entitled and which is not required to be returned to the Authority (in compliance with Law);

51.7.7 provide independently verifiable evidence that all Authority Data has been returned or irretrievably destroyed or disposed of;

51.7.8 only use a means of disposal or destruction previously agreed with the Authority in writing;

51.7.9 return to the Authority such of the following as is in the Supplier's possession or control:-

(a) all copies of the Authority Software and any other software licensed by the Authority to the Supplier under this Agreement;

(b) all materials created by the Supplier under this Agreement in which the IPRs are owned by the Authority;

(c) any parts of the IT Environment and any other equipment which belongs to the Authority; and

(d) any items that have been on--charged to the Authority, such as consumables;

51.7.10 vacate any Authority Premises unless access is required to continue to deliver the Services (or part thereof) and is approved in writing by the Authority; and

51.7.11 provide access during normal working hours or where otherwise agreed in writing to the Authority, any Service Recipient for up to twelve (12) months after the Partial Termination, expiry or termination of this Agreement to:-

(a) such information relating to the provision of the Services as remains in the possession or control of the Supplier; and

(b) such members of the Supplier Personnel as have been involved in the design, development and provision of the Services and who are still employed by the Supplier, provided that the Authority and/or the Replacement Supplier shall pay the reasonable costs of the Supplier actually incurred in responding to requests for access under this paragraph 3.2.

51.8 At the end of the Termination Assistance Period (or earlier if this does not adversely affect the Supplier's performance and/or delivery of the Services and the Termination Services and its compliance with the other provisions of this Schedule), each Party shall return to the other Party (or if requested, destroy or delete) all Confidential Information of the other Party in respect of the terminated Services and shall certify that it does not retain the other Party's Confidential Information save to the extent (and for the limited period) that such information needs to be retained by the Party in question for the purposes of providing or receiving any Services or Termination Services or for statutory compliance purposes.

51.9 Except where this Agreement provides otherwise, all licences, leases and authorisations granted by the Authority to the Supplier in relation to the provision of the terminated Services shall be terminated with effect from the end of the Termination Assistance Period.

52. ASSETS, SUB-CONTRACTS AND SOFTWARE

52.1 Following notice of termination or Partial Termination of this Agreement and during the Termination Assistance Period, the Supplier shall not, in respect of the terminated Services, without the Authority's prior written consent:-

52.1.1 terminate, enter into or vary any Sub-contract except to the extent that such change does not or will not affect the provision of Services, the Charges, or the delivery of the agreed Exit Plan;

52.1.2 (subject to normal maintenance requirements) make material modifications to, or dispose of, any existing Assets or acquire any new Assets; or

52.1.3 terminate, enter into or vary any licence for software in connection with the provision of the Services.

53. CHARGES

53.1 During the Termination Assistance Period (or for such shorter period as the Authority may require the Supplier to provide the Termination Services), the Authority shall pay the Charges to the Supplier in respect of the Termination Services in accordance with the rates set out in the Exit Plan (but shall not be required to pay costs in excess of the estimate set out in the Exit Plan). If the scope or timing of the Termination Services is changed and this results in a change to the costs of such Termination Services, the estimate may be varied in accordance with the Change Control Procedure.

53.2 Where the Authority requests an extension to the Termination Services beyond the Termination Assistance Period in accordance with paragraph 0:-

53.2.1 where more than six (6) months' notice is provided, the same rate as set out in the Exit Plan (or the Charges when not stated in the Exit Plan) shall be payable; and

53.2.2 where less than six (6) months' notice is provided, no more than 1.2 times the rate as set out in the Exit Plan (or the Charges when not stated in the Exit Plan) shall be payable.

53.3 For the purpose of calculating the costs of providing the Termination Services for inclusion in the Exit Plan or, if no Exit Plan has been agreed, the costs of providing Termination Services shall be determined in accordance with the Change Control Procedure.

53.4 Except as otherwise expressly specified in this Agreement, the Supplier shall not make any charges for the services provided by the Supplier pursuant to, and the Authority shall not be obliged to pay for costs incurred by the Supplier in relation to its compliance with, this Schedule including the preparation and implementation of the Exit Plan and any activities mutually agreed between the Parties to carry on after the expiry of the Termination Assistance Period.

APPENDIX 17

SCOPE OF THE TERMINATION SERVICES

54. The Termination Services to be provided by the Supplier shall include such of the following services as the Authority may specify:-

54.1 ceasing all non-critical Software changes (except where agreed in writing with the Authority);

54.2 notifying the Sub-contractors of procedures to be followed during the Termination Assistance Period and providing management to ensure these procedures are followed;

54.3 providing assistance and expertise as necessary to examine all operational and business processes (including all supporting documentation) in place and re-writing and implementing processes and procedures such that they are appropriate for use by the Authority and/or the Replacement Supplier after the end of the Termination Assistance Period;

54.4 delivering to the Authority the existing systems support profiles, monitoring or system logs, incident and problem tracking together with associated resolution documentation and status reports all relating to the twelve (12) month period immediately prior to the commencement of the Termination Services;

54.5 with respect to work in progress as at the end of the Termination Assistance Period, documenting the current status and stabilising for continuity during transition;

54.6 providing the Authority with any problem logs in the format agreed which have not previously been provided to the Authority;

54.7 agreeing with the Authority a handover plan for all of the Supplier's responsibilities as set out in the Security Management Plan;

54.8 in respect of the maintenance and support of the Supplier System, providing historical performance data for the previous twelve months;

54.9 assisting in the execution of a parallel operation of the maintenance and support of the Supplier System until the end of the Termination Assistance Period or as otherwise specified by the Authority (provided that the provision of these Services shall end on a date no later than the end of the Termination Assistance Period);

54.10 providing an information pack listing and describing the Services as configured, for use by the Authority in the procurement of the Replacement Services;

54.11 answering all reasonable questions from the Authority regarding the provision of the Services;

54.12 agreeing with the Authority, any Service Recipient a plan for the migration of the Authority Data to the Authority, any Service Recipient and/or the Replacement Supplier;

54.13 providing access to the Authority during the Termination Assistance Period and for a period not exceeding six (6) months afterwards for the purpose of the smooth transfer of the provision of the Services to the Authority, any Service Recipient and/or the Replacement Supplier:-

54.13.1 to information and documentation relating to the Transferring Services that is in the possession or control of the Supplier or its Sub-contractors (and the Supplier agrees and shall procure that its Sub-contractors do not destroy or dispose of that information within this period) including the right to take reasonable copies of that material; and

54.13.2 following reasonable notice and during the Supplier's normal business hours, to members of the Supplier Personnel who have been involved in the provision or management of the Services and who are still employed or engaged by the Supplier or its Sub-contractors;

54.14 knowledge transfer services, including:-

54.14.1 .

54.15 The Supplier shall:-

54.15.1 provide a documented plan relating to the training matters referred to in paragraph **Error! Reference source not found.** for agreement by the Authority at the time of termination or expiry of this Agreement;

54.15.2 co-operate fully in the execution of the handover plan agreed pursuant to paragraph 54.7, providing skills and expertise of a suitable standard; and

54.15.3 fully co-operate in the execution of the Authority Data migration plan agreed pursuant to paragraph 54.12, providing skills and expertise of a reasonably acceptable standard.

SCHEDULE 8.6

SERVICE CONTINUITY PLAN

Issue No:	Summary of Change:
V0.1	Version for issue with ITT

PART 1

SERVICE CONTINUITY PLAN

DEFINITIONS

In this Schedule, the definitions set out in Schedule 1 shall apply.

55. SERVICE CONTINUITY PLAN

55.1 The initial version of the Service Continuity Plan as at the Effective Date is set out at Appendix 1 of Part 1 to this Schedule 8.6 (*Service Continuity Plan*). The Service Continuity Plan details the processes and arrangements that the Supplier shall follow to:-

55.1.1 ensure continuity of the business processes and operations supported by the Services following any failure or disruption of any element of the Services (including where caused

by an Insolvency Event of the Supplier, any subcontractor and/or any Supplier Group member); and

55.1.2 the recovery of the Services in the event of a Disaster.

55.2 The Service Continuity Plan shall:-

55.2.1 be divided into four parts:-

(a) Part A which shall set out general principles applicable to the Service Continuity Plan;

(b) Part B which shall relate to business continuity (the "**Business Continuity Plan**");

(c) Part C which shall relate to disaster recovery (the "**Disaster Recovery Plan**");

55.2.2 unless otherwise required by the Authority in writing, be based upon and be consistent with the provisions of paragraphs 2, 2.1, 3 and 5. Where there is inconsistency in the plan versus what is required in this Schedule, the Schedule shall take precedence.

56. SERVICE CONTINUITY PLAN:- PART A - GENERAL PRINCIPLES AND REQUIREMENTS

56.1 Part A of the Service Continuity Plan shall:-

56.1.1 set out how the business continuity, disaster recovery elements of the plan link to each other;

56.1.2 provide details of how the invocation of any element of the Service Continuity Plan may impact upon the provision of the Services and any services provided to the Authority or any Service Recipient by a Related Service Provider;

56.1.3 contain an obligation upon the Supplier to liaise with the Authority and (at the Authority's request) any Related Service Provider with respect to issues concerning business continuity, disaster recovery where applicable;

56.1.4 detail how the Service Continuity Plan links and interoperates with any overarching and/or connected disaster recovery, business continuity plan of the Authority and any of its other Related Service Providers in each case as notified to the Supplier by the Authority from time to time;

56.1.5 contain a communication strategy including details of an incident and problem management service and advice and help desk facility which can be accessed via multi-channels (including but without limitation a web-site (with FAQs), e-mail, phone and fax) for both portable and desk top configurations, where required by the Authority;

56.1.6 contain a risk analysis, including:-

(a) failure or disruption scenarios and assessments and estimates of frequency of occurrence;

(b) identification of any potential single points of failure within the provision of the Services and processes for managing the risks arising therefrom and the steps to be taken by the Supplier to ensure that there are no such single points of failure;

(c) identification of risks arising from the interaction of the Services with the services provided by a Related Service Provider;

(d) a business impact analysis (detailing the impact on business processes and operations) of different anticipated failures or disruptions;

56.1.7 set out key contact details (including roles and responsibilities) for the Supplier (and any Sub-contractors) and for the Authority;

56.1.8 identify the procedures for reverting to "normal service";

56.1.9 set out method(s) of recovering or updating data collected (or which ought to have been collected) during a failure or disruption to ensure that there is no more than the accepted amount of data loss and to preserve data integrity;

56.1.10 identify the responsibilities (if any) that the Authority has agreed it will assume in the event of the invocation of the Service Continuity Plan; and

56.1.11 provide for the provision of technical advice and assistance to key contacts at the Authority as notified by the Authority from time to time to inform decisions in support of the Authority's business continuity plans.

56.2 The Service Continuity Plan shall be designed so as to ensure that:-

56.2.1 the Services are provided in accordance with this Agreement at all times during and after the invocation of the Service Continuity Plan;

56.2.2 the adverse impact of any Disaster, service failure, pandemic (including the impacts of COVID-19 (or similar)), , or disruption on the operations of the Authority and the Service Recipients, is minimal as far as reasonably possible;

56.2.3 it complies with the relevant provisions of ISO/IEC27002 and all other industry standards from time to time in force; and

56.2.4 there is a process for the management of disaster recovery testing detailed in the Service Continuity Plan.

56.3 The Service Continuity Plan shall be upgradeable and sufficiently flexible to support any changes to the provision of the Services, to the business processes facilitated by and the business operations supported by the provision by the Supplier of the Services, and/or changes to the Supplier Group structure.

56.4 The Supplier shall not be entitled to any relief from its obligations under the Performance Indicators or to any increase in the Charges to the extent that a Disaster occurs as a consequence of any breach by the Supplier of this Agreement.

57. SERVICE CONTINUITY PLAN:- PART B - BUSINESS CONTINUITY PRINCIPLES AND CONTENTS

57.1 The Business Continuity Plan shall set out the arrangements that are to be invoked to ensure that the business processes and operations facilitated by the provision by the Supplier of the Services and remain supported and to ensure continuity of the business operations supported by the provision of the Services including, unless the Authority expressly states otherwise in writing:-

57.1.1 the alternative processes (including business processes), options and responsibilities that may be adopted in the event of a failure in or disruption to the provision by the Supplier of the Services; and

57.1.2 the steps to be taken by the Supplier upon resumption of the provision by the Supplier of the Services in order to address any prevailing effect of the failure or disruption including a root cause analysis of the failure or disruption.

57.2 The Business Continuity Plan shall:-

57.2.1 address the various possible levels of failures of or disruptions to the provision by the Supplier of the Services;

57.2.2 set out the services to be provided and the steps to be taken to remedy the different levels of failures of and disruption to the provision by the Supplier of the Services (such services and steps, the "**Business Continuity Services**");

57.2.3 specify any applicable Performance Indicators with respect to the provision of the Business Continuity Services and details of any agreed relaxation to the Performance Indicators in respect of other Services during any period of invocation of the Business Continuity Plan; and

57.2.4 clearly set out the conditions and/or circumstances under which the Business Continuity Plan is invoked.

58. SERVICE CONTINUITY PLAN:- PART C - DISASTER RECOVERY PRINCIPLES AND CONTENT

58.1 The Disaster Recovery Plan shall be designed so as to ensure that upon the occurrence of a Disaster the Supplier ensures continuity of the business operations of the Authority and the Service Recipients supported by the provision by the Supplier of the Services following any Disaster or during any period of service failure or disruption with, as far as reasonably possible, minimal adverse impact.

58.2 The Disaster Recovery Plan shall be invoked only upon the occurrence of a Disaster.

58.3 The Disaster Recovery Plan shall include the following:-

58.3.1 the technical design and build specification of the Disaster Recovery System;

58.3.2 details of the procedures and processes to be put in place by the Supplier in relation to the Disaster Recovery System and the provision of the Disaster Recovery Services and any testing of the same including the following:-

(a) data centre and disaster recovery site audits;

(b) backup methodology and details of the Supplier's approach to data back-up and data verification;

(c) identification of all potential disaster scenarios;

(d) risk analysis;

(e) documentation of processes and procedures;

(f) hardware configuration details;

(g) network planning including details of all relevant data networks and communication links;

(h) invocation rules;

(i) Service recovery procedures; and

(j) steps to be taken upon resumption of the provision of the Services to address any prevailing effect of the failure or disruption of the provision of the Services;

58.3.3 any applicable Performance Indicators with respect to the provision of the Disaster Recovery Services and details of any agreed relaxation to the Performance Indicators in respect of other Services during any period of invocation of the Disaster Recovery Plan;

58.3.4 details of how the Supplier shall ensure compliance with security standards set out in Schedule 2.4 (Security Management) ensuring that compliance is maintained for any period during which the Disaster Recovery Plan is invoked;

58.3.5 access controls to any disaster recovery sites used by the Supplier in relation to its obligations pursuant to this Schedule; and

58.3.6 testing and management arrangements.

59. REVIEW AND AMENDMENT OF THE SERVICE CONTINUITY PLAN

59.1 The Supplier shall review and update the Service Continuity Plan (and the risk analysis on which it is based):-

59.1.1 on a regular basis and as a minimum once every six (6) months;

59.1.2 where the Authority requests any additional reviews (over and above those provided for in paragraphs 1 to 8) by notifying the Supplier to such effect in writing, whereupon the Supplier shall promptly conduct such reviews in accordance with the Authority's written requirements. Prior to starting its review, the Supplier shall provide an accurate written estimate of the total costs payable by the Authority for the Authority's approval. The costs of both Parties of any such additional reviews shall be met by the Authority except that the Supplier shall not be entitled to charge the Authority for any costs that it may incur above any estimate without the Authority's prior written approval.

59.2 Each review of the Service Continuity Plan pursuant to paragraph 0 shall be a review of the procedures and methodologies set out in the Service Continuity Plan and shall assess their suitability having regard to any change to the provision of the Services or any underlying business processes and operations facilitated by or supported by the provision of the Services which have taken place since the later of the original approval of the Service Continuity Plan or the last review of the Service Continuity Plan and shall also have regard to any occurrence of any event since that date (or the likelihood of any such event taking place in the foreseeable future) which may increase the likelihood of the need to invoke the Service Continuity Plan. The review shall be completed by the Supplier within the period required by the Service Continuity Plan or, if no such period is required, within such period as the Authority shall reasonably require. The Supplier shall, within twenty (20) Working Days of the conclusion of each such review of the Service Continuity Plan, provide to the Authority a report (a "**Review Report**") setting out:-

59.2.1 the findings of the review;

59.2.2 any changes in the risk profile associated with the provision of the Services; and

59.2.3 the Supplier's proposals (the "**Supplier's Proposals**") for addressing any changes in the risk profile and its proposals for amendments to the Service Continuity Plan following the review detailing the impact (if any and to the extent that the Supplier can reasonably be expected to be aware of the same) that the implementation of such proposals may have on any services or systems provided by a third party.

59.3 Following receipt of the Review Report and the Supplier's Proposals, the Authority shall:-

59.3.1 review and comment on the Review Report and the Supplier's Proposals as soon as reasonably practicable; and

59.3.2 notify the Supplier in writing that it approves or rejects the Review Report and the Supplier's Proposals no later than twenty (20) Working Days after the date on which they are first delivered to the Authority.

59.4 If the Authority rejects the Review Report and/or the Supplier's Proposals:-

59.4.1 the Authority shall inform the Supplier in writing of its reasons for its rejection; and

59.4.2 the Supplier shall then revise the Review Report and/or the Supplier's Proposals as the case may be (taking reasonable account of the Authority's comments and carrying out any necessary actions in connection with the revision) and shall re-submit a revised Review Report and/or revised Supplier's Proposals to the Authority for the Authority's approval within ten (10) Working Days of the date of the Authority's notice of rejection. The provisions of paragraph 10 and this paragraph 54.12 shall apply again to any resubmitted Review Report and Supplier's Proposals up to a maximum of two (2) times (unless otherwise agreed in writing by the Authority), provided that either Party may refer any disputed matters for resolution by the Dispute Resolution Procedure at any time (or if the procedure set out in paragraph 10 and this paragraph 54.12 has been exhausted in accordance the terms of this paragraph 59.4.2).

59.5 The Supplier shall as soon as is reasonably practicable after receiving the Authority's approval of the Supplier's Proposals (having regard to the significance of any risks highlighted in the Review Report) effect any change in its practices or procedures necessary so as to give effect to the Supplier's Proposals. Any such change shall be at the Supplier's expense unless it can be reasonably shown that the changes are required because of a material change to the risk profile of the provision of the Services.

60. TESTING OF THE SERVICE CONTINUITY PLAN

60.1 The Supplier shall test the Service Continuity Plan on a regular basis (and in any event not less than once in every Contract Year). Subject to paragraph 5.7.1, the Authority may require the Supplier to conduct additional tests of some or all aspects of the Service Continuity Plan at any time where the Authority considers it necessary, including where there has been any change to the provision of the Services or any underlying business processes, or on the occurrence of any event which may increase the likelihood of the need to implement the Service Continuity Plan.

60.2 If the Authority requires an additional test of the Service Continuity Plan, it shall give the Supplier written notice and the Supplier shall conduct the test in accordance with the Authority's requirements and the relevant provisions of the Service Continuity Plan. The Supplier's costs of the additional test (as agreed in advance with the Authority) shall be borne by the Authority unless the Service Continuity Plan fails the additional test in which case the Supplier's costs of that failed test shall be borne by the Supplier.

60.3 The Supplier shall ensure that any use by it or any Sub-contractor of "live" data in such testing is first approved with the Authority. Copies of live test data used in any such testing shall be (if so required by the Authority) destroyed or returned to the Authority on completion of the test.

60.4 The Supplier shall, within twenty (20) Working Days of the conclusion of each test, provide to the Authority a report setting out:-

60.4.1 the outcome of the test;

60.4.2 any failures in the Service Continuity Plan (including the Service Continuity Plan's procedures) revealed by the test; and

60.4.3 the Supplier's proposals for remedying any such failures.

60.5 Following each test, the Supplier shall take all measures requested by the Authority, (including requests for the re-testing of the Service Continuity Plan) to remedy any failures in the Service Continuity Plan and such remedial activity and re-testing shall be completed by the Supplier, at no additional cost to the Authority, by the date reasonably required by the Authority and set out in such notice.

60.6 For the avoidance of doubt, the carrying out of a test of the Service Continuity Plan (including a test of the Service Continuity Plan's procedures) shall not relieve the Supplier of any of its obligations under this Agreement.

61. INVOCATION OF THE SERVICE CONTINUITY PLAN

61.1 In the event of a loss of any critical part of the Service or a Disaster, the Supplier shall immediately invoke the business continuity and disaster recovery provisions in the Service Continuity Plan, including any linked elements in other parts of the Service Continuity Plan (and shall inform the Authority promptly of such invocation). In all other instances the Supplier shall invoke the business continuity and disaster recovery plan elements only with the prior consent of the Authority.

APPENDIX 1

Service Continuity Plan

[Redacted For Publication]

SCHEDULE 8.7

CONDUCT OF CLAIMS

Issue No:	Summary of Change:
V0.1	Initial version

62. **INDEMNITIES**

62.1 This Schedule shall apply to the conduct, by a Party from whom an indemnity is sought under this Agreement (the "**Indemnifier**"), of claims made by a third person against a party having (or claiming to have) the benefit of the indemnity (the "**Beneficiary**").

62.2 If the Beneficiary receives any notice of any claim for which it appears that the Beneficiary is, or may become, entitled to indemnification under this Agreement (a "**Claim**"), the Beneficiary shall give notice in writing to the Indemnifier as soon as reasonably practicable and in any event within ten (10) Working Days of receipt of the same.

62.3 Subject to paragraph 1.2, on the giving of a notice by the Beneficiary, where it appears that the Beneficiary is or may be entitled to indemnification from the Indemnifier in respect of all (but not part only) of the liability arising out of the Claim, the Indemnifier shall (subject to providing the Beneficiary with a secured indemnity to its reasonable satisfaction against all costs and expenses that it may incur by reason of such action) be entitled to dispute the Claim in the name of the Beneficiary at the Indemnifier's own expense and take conduct of any defence, dispute, compromise or appeal of the Claim and of any incidental negotiations relating to the Claim. If the Indemnifier does elect to conduct the Claim, the Beneficiary shall give the Indemnifier all reasonable cooperation, access and assistance for the purposes of such Claim and, subject to paragraph 0, the Beneficiary shall not make any admission which could be prejudicial to the defence or settlement of the Claim without the prior written consent of the Indemnifier.

62.4 With respect to any Claim conducted by the Indemnifier pursuant to paragraph 1.1.1:-

62.4.1 the Indemnifier shall keep the Beneficiary fully informed and consult with it about material elements of the conduct of the Claim;

62.4.2 the Indemnifier shall not bring the name of the Beneficiary into disrepute;

62.4.3 the Indemnifier shall not pay or settle such Claim without the prior written consent of the Beneficiary, such consent not to be unreasonably withheld or delayed; and

62.4.4 the Indemnifier shall conduct the Claim with all due diligence.

62.5 The Beneficiary shall be entitled to have conduct of the Claim and shall be free to pay or settle any Claim on such terms as it thinks fit and without prejudice to its rights and remedies under this Agreement if:-

62.5.1 the Indemnifier is not entitled to take conduct of the Claim in accordance with paragraph 1.1.1;

62.5.2 the Indemnifier fails to notify the Beneficiary in writing of its intention to take conduct of the relevant Claim within ten (10) Working Days of the notice from the Beneficiary or if the Indemnifier notifies the Beneficiary in writing that it does not intend to take conduct of the Claim; or

62.5.3 the Indemnifier fails to comply in any material respect with the provisions of paragraph 1.4.

63. SENSITIVE CLAIMS

63.1 With respect to any Claim which the Beneficiary, acting reasonably, considers is likely to have an adverse impact on the general public's perception of the Beneficiary (a "**Sensitive Claim**"), the Indemnifier shall be entitled to take conduct of any defence, dispute, compromise or appeal of the Sensitive Claim only with the Beneficiary's prior written consent. If the Beneficiary withholds such consent and elects to conduct the defence, dispute, compromise or appeal of the Sensitive Claim itself, it shall conduct the Sensitive Claim with all due diligence and if it fails to do so, the Indemnifier shall only be liable to indemnify the Beneficiary in respect of that amount which would have been recoverable by the Beneficiary had it conducted the Sensitive Claim with all due diligence.

63.2 The Beneficiary shall be free at any time to give written notice to the Indemnifier that it is retaining or taking over (as the case may be) the conduct of any Claim, to which paragraph 1.1.1 applies if, in the reasonable opinion of the Beneficiary, the Claim is, or has become, a Sensitive Claim.

64. RECOVERY OF SUMS

64.1 If the Indemnifier pays to the Beneficiary an amount in respect of an indemnity and the Beneficiary subsequently recovers (whether by payment, discount, credit, saving, relief or other benefit or otherwise) a sum which is directly referable to the fact, matter, event or circumstances giving rise to the Claim, the Beneficiary shall forthwith repay to the Indemnifier whichever is the lesser of:-

64.1.1 an amount equal to the sum recovered (or the value of the discount, credit, saving, relief, other benefit or amount otherwise obtained) less any out-of-pocket costs and expenses properly incurred by the Beneficiary in recovering or obtaining the same; and

64.1.2 the amount paid to the Beneficiary by the Indemnifier in respect of the Claim under the relevant indemnity.

65. MITIGATION

Each of the Authority and the Supplier shall at all times take all reasonable steps to minimise and mitigate any loss for which the relevant Party is entitled to bring a claim against the other Party pursuant to the indemnities in this Schedule.

SCHEDULE 9.1

STAFF TRANSFER

Issue No:	Summary of Change:
V0.1	Version for issue with ITT

66. **DEFINITIONS**

In this Schedule, the definitions set out in Schedule 1 shall apply.-

67. **INTERPRETATION**

Where a provision in this Schedule imposes an obligation on the Supplier to provide an indemnity, undertaking or warranty, the Supplier shall procure that each of its Sub-contractors shall comply with such obligation and provide such indemnity, undertaking or warranty to the Authority, Former Supplier Replacement Supplier or Replacement Sub-contractor, as the case may be.

PART A [NOT USED]

PART B [NOT USED]

PART C

NO TRANSFER OF EMPLOYEES AT COMMENCEMENT OF SERVICES

68. **PROCEDURE IN THE EVENT OF TRANSFER**

68.1 The Authority and the Supplier agree that the commencement of the provision of the Services or of any part of the Services will not be a Relevant Transfer in relation to any employees of the Authority and/or any Former Supplier.

68.2 If any employee of the Authority and/or a Former Supplier claims, or it is determined in relation to any employee of the Authority and/or a Former Supplier, that his/her contract of employment has been transferred from the Authority and/or the Former Supplier to the Supplier and/or any Sub-contractor pursuant to the Employment Regulations or the Acquired Rights Directive then:-

68.2.1 the Supplier shall, and shall procure that the relevant Sub-contractor shall, within five (5) Working Days of becoming aware of that fact, give notice in writing to the Authority and, where required by the Authority, give notice to the Former Supplier; and

68.2.2 the Authority and/or the Former Supplier may offer (or may procure that a third party may offer) employment to such person within fifteen (15) Working Days of the notification by the Supplier or the Sub-contractor (as appropriate) or take such other reasonable steps as the Authority or Former Supplier (as the case may be) considers appropriate to deal with the matter provided always that such steps are in compliance with applicable Law.

68.3 If an offer referred to in paragraph 3.2.2 is accepted (or if the situation has otherwise been resolved by the Authority and/or the Former Supplier), the Supplier shall, or shall procure that the Sub-contractor shall, immediately release the person from his/her employment or alleged employment.

68.4 If by the end of the fifteenth (15) Working Day period specified in paragraph 3.2.2:-

68.4.1 no such offer of employment has been made;

68.4.2 such offer has been made but not accepted; or

68.4.3 the situation has not otherwise been resolved,

the Supplier and/or the Sub-contractor may within five (5) Working Days give notice to terminate the employment or alleged employment of such person.

69. **INDEMNITIES**

69.1 Subject to the Supplier and/or the relevant Sub-contractor acting in accordance with the provisions of paragraphs 3.1 to 3.4 and in accordance with all applicable employment procedures set out in applicable Law and subject also to paragraph 3.10, the Authority shall:-

69.1.1 indemnify the Supplier and/or the relevant Sub-contractor against all Employee Liabilities arising out of the termination of the employment of any employees of the Authority referred to in paragraph 3.2 made pursuant to the provisions of paragraph 3.4 provided that the Supplier takes all reasonable steps to minimise any such Employee Liabilities; and

69.1.2 procure that the Former Supplier indemnifies the Supplier against all Employee Liabilities arising out of termination of the employment of the employees of the Former Supplier referred to in paragraph 3.2 made pursuant to the provisions of paragraph 3.4 provided that the Supplier takes, or shall procure that the relevant Sub-contractor takes, all reasonable steps to minimise any such Employee Liabilities.

69.2 If any such person as is described in paragraph 3.2 is neither re-employed by the Authority and/or the Former Supplier as appropriate nor dismissed by the Supplier and/or any Sub-contractor within the fifteenth (15) Working Day period referred to in paragraph 3.4 such person shall be treated as having transferred to the Supplier and/or the Sub-contractor (as appropriate) and the Supplier shall, or shall procure that the Sub-contractor shall, comply with such obligations as may be imposed upon it under Law.

69.3 Where any person remains employed by the Supplier and/or any Sub-contractor pursuant to paragraph 4, all Employee Liabilities in relation to such employee shall remain with the Supplier and/or the Sub-contractor and the Supplier shall indemnify the Authority and any Former Supplier, and shall procure that the Sub-contractor shall indemnify the Authority and any Former Supplier, against any Employee Liabilities that either of them may incur in respect of any such employees of the Supplier and/or employees of the Sub-contractor.

69.4 The indemnities in paragraph 4.10:-

69.4.1 shall not apply to:-

(a) any claim for:-

(i) discrimination, including on the grounds of sex, race, disability, age, gender reassignment, marriage or civil partnership, pregnancy and maternity or sexual orientation, religion or belief; or

(ii) equal pay or compensation for less favourable treatment of part-time workers or fixed--term employees,

in any case in relation to any alleged act or omission of the Supplier and/or any Sub-contractor; or

(b) any claim that the termination of employment was unfair because the Supplier and/or any Sub-contractor neglected to follow a fair dismissal procedure; and

69.4.2 shall apply only where the notification referred to in paragraph 3.2.1 is made by the Supplier and/or any Sub-contractor to the Authority and, if applicable, Former Supplier within 6 months of the Effective Date.

PART D [NOT USED]

SCHEDULE 10

STANDARD CONTRACTUAL CLAUSES AND INTERNATIONAL DATA TRANSFER ADDENDUM

ANNEX

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A. (hereinafter each "data exporter"), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each "data importer")

have agreed to these standard contractual clauses (hereinafter: "Clauses").

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g);

(iii) Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 - Modules One, Two and Three: Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 - Optional

Docking clause

(d) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(e) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(f) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

MODULE ONE: Transfer controller to controller

8.1 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B. It may only process the personal data for another purpose:

(i) where it has obtained the data subject's prior consent;

(ii) where necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iii) where necessary in order to protect the vital interests of the data subject or of another natural person.

8.2 Transparency

(g) In order to enable data subjects to effectively exercise their rights pursuant to Clause 10, the data importer shall inform them, either directly or through the data exporter:

(i) of its identity and contact details;

(ii) of the categories of personal data processed;

(iii) of the right to obtain a copy of these Clauses;

(iv) where it intends to onward transfer the personal data to any third party/ies, of the recipient or categories of recipients (as appropriate with a view to providing meaningful information), the purpose of such onward transfer and the ground therefore pursuant to Clause 8.7.

(h) Paragraph (a) shall not apply where the data subject already has the information, including when such information has already been provided by the data exporter, or providing the information proves impossible or would involve a disproportionate effort for the data importer. In the latter case, the data importer shall, to the extent possible, make the information publicly available.

(i) On request, the Parties shall make a copy of these Clauses, including the Appendix as completed by them, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the Parties may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

(j) Paragraphs (a) to (c) are without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.3 Accuracy and data minimisation

(k) Each Party shall ensure that the personal data is accurate and, where necessary, kept up to date. The data importer shall take every reasonable step to ensure that personal data that is inaccurate, having regard to the purpose(s) of processing, is erased or rectified without delay.

(l) If one of the Parties becomes aware that the personal data it has transferred or received is inaccurate, or has become outdated, it shall inform the other Party without undue delay.

(m) The data importer shall ensure that the personal data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of processing.

8.4 Storage limitation

The data importer shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed. It shall put in place appropriate technical or organisational measures to ensure compliance with this obligation, including erasure or anonymisation of the data and all back-ups at the end of the retention period.

8.5 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the personal data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter "personal data breach"). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

(b) The Parties have agreed on the technical and organisational measures set out in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(c) The data importer shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(d) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the personal data breach, including measures to mitigate its possible adverse effects.

(e) In case of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the data importer shall without undue delay notify both the data exporter and the competent supervisory authority pursuant to Clause 13. Such notification shall contain i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), ii) its likely consequences, iii) the measures taken or proposed to address the breach, and iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible for the data importer to provide all the information at the same time, it may do so in phases without undue further delay.

(f) In case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the data importer shall also notify without undue delay the data subjects concerned of the personal data breach and its nature, if necessary in cooperation with the data exporter, together with the information referred to in paragraph (e), points ii) to iv), unless the data importer has implemented measures to significantly reduce the risk to the rights or freedoms of natural persons, or notification would involve disproportionate efforts. In the latter case, the data importer shall instead issue a public communication or take a similar measure to inform the public of the personal data breach.

(g) The data importer shall document all relevant facts relating to the personal data breach, including its effects and any remedial action taken, and keep a record thereof.

8.6 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences (hereinafter "sensitive data"), the data importer shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved. This may include restricting the personnel permitted to access the

personal data, additional security measures (such as pseudonymisation) and/or additional restrictions with respect to further disclosure.

8.7 Onward transfers

The data importer shall not disclose the personal data to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter "onward transfer") unless the third party is or agrees to be bound by these Clauses, under the appropriate Module. Otherwise, an onward transfer by the data importer may only take place if:

(i) it is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679 with respect to the processing in question;

(iii) the third party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter;

(iv) it is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings;

(v) it is necessary in order to protect the vital interests of the data subject or of another natural person; or

(vi) where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject for an onward transfer in a specific situation, after having informed him/her of its purpose(s), the identity of the recipient and the possible risks of such transfer to him/her due to the lack of appropriate data protection safeguards. In this case, the data importer shall inform the data exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the data subject.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.8 Processing under the authority of the data importer

The data importer shall ensure that any person acting under its authority, including a processor, processes the data only on its instructions.

8.9 Documentation and compliance

(a) Each Party shall be able to demonstrate compliance with its obligations under these Clauses. In particular, the data importer shall keep appropriate documentation of the processing activities carried out under its responsibility.

(b) The data importer shall make such documentation available to the competent supervisory authority on request.

MODULE TWO: Transfer controller to processor

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful

destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter "personal data breach"). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter

"onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

MODULE TWO: Transfer controller to processor

OPTION 2: GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 14 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data

exporter with the information necessary to enable the data exporter to exercise its right to object.

(a) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(b) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(c) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(d) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

MODULE ONE: Transfer controller to controller

(a) The data importer, where relevant with the assistance of the data exporter, shall deal with any enquiries and requests it receives from a data subject relating to the processing of his/her personal data and the exercise of his/her rights under these Clauses without undue delay and at the latest within one month of the receipt of the enquiry or request. The data importer shall take appropriate measures to facilitate such enquiries, requests and the exercise of data subject rights. Any information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.

(b) In particular, upon request by the data subject the data importer shall, free of charge:

(i) provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in Annex I; if personal data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing meaningful information) to which the personal data has been or will be onward transferred, the purpose of such onward transfers and their ground pursuant to Clause 8.7; and provide information on the right to lodge a complaint with a supervisory authority in accordance with Clause 12(c)(i);

(ii) rectify inaccurate or incomplete data concerning the data subject;

(iii) erase personal data concerning the data subject if such data is being or has been processed in violation of any of these Clauses ensuring third-party beneficiary rights, or if the data subject withdraws the consent on which the processing is based.

(c) Where the data importer processes the personal data for direct marketing purposes, it shall cease processing for such purposes if the data subject objects to it.

(d) The data importer shall not make a decision based solely on the automated processing of the personal data transferred (hereinafter "automated decision"), which would produce legal effects concerning the data subject or similarly significantly affect him / her, unless with the explicit consent of the data subject or if authorised to do so under the laws of the country of destination, provided that such laws lays down suitable measures to safeguard the data subject's rights and legitimate interests. In this case, the data importer shall, where necessary in cooperation with the data exporter:

(i) inform the data subject about the envisaged automated decision, the envisaged consequences and the logic involved; and

(ii) implement suitable safeguards, at least by enabling the data subject to contest the decision, express his/her point of view and obtain review by a human being.

(e) Where requests from a data subject are excessive, in particular because of their repetitive character, the data importer may either charge a reasonable fee taking into account the administrative costs of granting the request or refuse to act on the request.

(f) The data importer may refuse a data subject's request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a democratic society to protect one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679.

(g) If the data importer intends to refuse a data subject's request, it shall inform the data subject of the reasons for the refusal and the possibility of lodging a complaint with the competent supervisory authority and/or seeking judicial redress.

MODULE TWO: Transfer controller to processor

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

(d) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

(a) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(b) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(c) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(d) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(e) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

MODULE ONE: Transfer controller to controller

MODULE FOUR: Transfer processor to controller

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.

(c) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(d) The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(e) The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

MODULE TWO: Transfer controller to processor

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

(a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within

the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation [. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal

data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) For Modules One and Two: Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland (*specify Member State*).

Clause 18

Choice of forum and jurisdiction

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Ireland.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

ANNEX I

A. LIST OF PARTIES

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

Data exporter(s):

1. Name: NUCLEAR DECOMMISSIONING AUTHORITY

Address: Herdus House, Westlakes Science Park, Moor Row, Cumbria CA24 3HU

Contact person's name, position and contact details: **[Redacted For Publication]**

Activities relevant to the data transferred under these Clauses:

See below at paragraph B under "Nature and purpose of the processing"

[Redacted For Publication]

21/11/2022

See signature blocks of the NDA COMMERCIAL SYSTEMS PROCUREMENT agreement

Role: Controller

2.Name: LLW Repository T/A NWS

Address: … Pelham House, Pelham Drive, Calderbridge, Cumbria, CA20 1DB

Activities relevant to the data transferred under these Clauses: See below at paragraph B under "Nature and purpose of the processing"

[Redacted For Publication]

18/11/2022

Role: Controller

3. Nuclear Transport Solutions

Address: Herdus House, Westlakes Science & Technology Park, Moor Row, Cumbria, CA24 3HU

Activities relevant to the data transferred under these Clauses: See below at paragraph B under "Nature and purpose of the processing"

Signature and date: … 18/11/2022

Role: Controller

[Redacted For Publication]

Procurement Manager (Corporate, People & IT)

4. Name: Sellafield Limited

Address: Hinton House Birchwood Park Avenue, Risley, Warrington, Cheshire, United Kingdom, WA3 6GR

Activities relevant to the data transferred under these Clauses: See below at paragraph B under "Nature and purpose of the processing"

Signature and date: 21/11/2022

[Redacted For Publication]

Role: Controller

5. Name: Dounreay Site Restoration Limited

Address: Building D2003, Dounreay, Thurso, Caithness, KW14 7TZ

Activities relevant to the data transferred under these Clauses: See below at paragraph B under "Nature and purpose of the processing"

Signature and date: …

Role: Controller

16/11/2022

[Redacted For Publication]

Head of Commercial Services, Dounreay

6. Name: Magnox Limited

Address: Oldbury Technical Centre, Oldbury Naite, Thornbury, South Gloucestershire, England, BS35 1RQ

Activities relevant to the data transferred under these Clauses: See below at paragraph B under "Nature and purpose of the processing"

[Redacted For Publication]

17 November 2022

Role: Controller

7. Name: RWM Limited T/A NWS

Address: … Pelham House, Pelham Drive, Calderbridge, Cumbria, CA20 1DB

Activities relevant to the data transferred under these Clauses: See below at paragraph B under "Nature and purpose of the processing"

[Redacted For Publication]

16/11/2022

Role: Controller

Data importer(s):

1. Name: RESILINC CORPORATION

Address: 1525 McCarthy Blvd., Suite 1122, Milpitas, CA 95035

Contact person's name, position and contact details:

[Redacted For Publication]

Activities relevant to the data transferred under these Clauses: See below at paragraph B under "Nature and purpose of the processing"

Signature and date: See Signature blocks of the NDA COMMERCIAL SYSTEMS PROCUREMENT agreement

[Redacted For Publication]

Role (controller/processor): Processor

MODULE ONE: Transfer controller to controller

Controller

MODULE TWO: Transfer controller to processor

Processor

B. DESCRIPTION OF TRANSFER

MODULE ONE: Transfer controller to controller

Categories of data subjects whose personal data is transferred:

Employees of the Exporters

Categories of personal data transferred:

Name, email, phone number, job title

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures:

N/A

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis):

Continuous

Nature and purpose of the processing:

(a) administer and provide the Services; (b) request and receive the Services; (c) compile, dispatch and manage the payment of invoices relating to the Services; (d) manage the Agreement and resolve any disputes relating to it; (e) respond and/or raise general queries relating to the Services; and (f) comply with their respective regulatory and other compliance obligations

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:

The term of the services agreement agreement between Exporter A and Importer

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:

N/A

MODULE TWO: Transfer controller to processor

Categories of data subjects whose personal data is transferred:

Employees and Directors of companies that supply goods and services to the Exporters

Categories of personal data transferred:

Name, email, phone number

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures:

N/A

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis):

Continuous

Nature and purpose of the processing:

Personal data is required to enable the Importer to provide supply chain risk management and mapping services, for example, contact details for key contacts at the Exporters' suppliers will be processed to enable the Exporter's personnel to readily locate such details

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:

The term of the NDA COMMERCIAL SYSTEMS PROCUREMENT agreement between Exporter 1 and the Importer

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:

Sub processor name: IBM Cloud

Purpose of processing: Only for storage of data. The Supplier Solution is hosted on IBM Cloud to store data.

Types of Personal Information shared with the sub processor: See above under "Categories of data subjects whose personal data is transferred"

Term: The term of the NDA COMMERCIAL SYSTEMS PROCUREMENT agreement between Exporter 1 and the Importer

C. COMPETENT SUPERVISORY AUTHORITY

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

Identify the competent supervisory authority/ies in accordance with Clause 13:

The Irish Data Protection Commission

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

EXPLANATORY NOTE:

The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Internet-facing firewalls to restrict access from the internet to the required ports only.

System hardening measures are in place to reduce the systems surface of vulnerability.

Security monitoring sytems in place to respond to network/system/application events.

Application access control ensuring access to the solution and data is only accessible to authenticated users.

Anti-virus and malware detection ststems in place to protect network/system security.

Data encryption measures in place to protect data in transit between site and IBM cloud.

User management and restricted system access.

Physical security and access measures to protect critical facilities from unauthorised physcial access.

All staff shall undertake annual security awareness training. This process shall be audited and monitered by manaagement.

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter:

See response immediately above.

ANNEX III – LIST OF SUB-PROCESSORS

MODULE TWO: Transfer controller to processor

EXPLANATORY NOTE:

This Annex must be completed for Modules Two and Three, in case of the specific authorisation of sub-processors (Clause 9(a), Option 1).

The controller has authorised the use of the following sub-processors:

1. Name: IBM Cloud

Purpose of processing: Only for storage of data. The Supplier Solution is hosted on IBM Cloud to store data.

Types of Personal Information shared with the sub processor - See above at Annex I Part B under "Categories of data subjects whose personal data is transferred"

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

VERSION B1.0, in force 21 March 2022

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

Part 1: Tables

TABLE 1: PARTIES

Start date		
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	**Exporter A** Full legal name: NUCLEAR DECOMMISSIONING AUTHORITY Main address (if a company registered address): Herdus House, Westlakes Science Park, Moor Row, Cumbria CA24 3HU **EXPORTER B** Full legal name: Nuclear Waste Services Main address (if a company registered address): Pelham House, Pelham Drive, Calderbridge, Cumbria, CA20 1DB **EXPORTER C** Full legal name: Nuclear Transport Solutions Main address (if a company registered address): Herdus House, Westlakes Science Park, Moor Row, Cumbria CA24 3HU **EXPORTER D** Full legal name: Sellafield Limited Main address (if a company registered address): Hinton House Birchwood	Full legal name: RESILINC CORPORATION Main address (if a company registered address): 1525 McCarthy Blvd., Suite 1122, Milpitas, CA 95035

	Park Avenue, Risley, Warrington, Cheshire, United Kingdom, WA3 6GR Official registration number (if any) (company number or similar identifier): 01002607 **EXPORTER E** Full legal name: Dounreay Site Restoration Limited Trading name (if different): Main address (if a company registered address): Building D2003, Dounreay, Thurso, Caithness, KW14 7TZ Official registration number (if any) (company number or similar identifier): SC307493 **EXPORTER F** Full legal name: Magnox Limited Trading name (if different): Main address (if a company registered address): Oldbury Technical Centre, Oldbury Naite, Thornbury, South Gloucestershire, England, BS35 1RQ Official registration number (if any) (company number or similar identifier): 02264251	
Key Contact	Full Name (optional): **[Redacted for Publication]**	Full Name (optional): **[Redacted for Publication]**
Signature (if required for the purposes of Section 2)	Not required – see clause 22.6 of the NDA COMMERCIAL SYSTEMS PROCUREMENT between Exporter A and the Importer	Not required – see clause 22.6 of the NDA COMMERCIAL SYSTEMS PROCUREMENT between Exporter A and the Importer

TABLE 2: SELECTED SCCS, MODULES AND SELECTED CLAUSES

Addendum EU SCCs	☐ The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date:

	Reference (if any): Other identifier (if any): Or X the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:

Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1	yes	yes	No			
2	yes	yes	No	General	14 days	
3						
4						

TABLE 3: APPENDIX INFORMATION

"**Appendix Information**" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: page 22

Annex 1B: Description of Transfer: page 23

Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: page 25

Annex III: List of Sub processors (Modules 2 and 3 only): page 27

TABLE 4: ENDING THIS ADDENDUM WHEN THE APPROVED ADDENDUM CHANGES

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: ☐ Importer ☐ Exporter X neither Party

Part 2: Mandatory Clauses

Entering into this Addendum

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.

2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this Addendum

3. Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.

UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

4. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.

6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

7. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.

10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.

11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

INCORPORATION OF AND CHANGES TO THE EU SCCS

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

    a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

    b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and

    c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.

14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.

15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:

    a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;

    b. In Clause 2, delete the words:

    "and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679";

    c. Clause 6 (Description of the transfer(s)) is replaced with:

    "The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";

    d. Clause 8.7(i) of Module 1 is replaced with:

    "it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";

    e. Clause 8.8(i) of Modules 2 and 3 is replaced with:

    "the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

    f. References to "Regulation (EU) 2016/679", "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

    g. References to Regulation (EU) 2018/1725 are removed;

h. References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";

i. The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";

j. Clause 13(a) and Part C of Annex I are not used;

k. The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";

l. In Clause 16(e), subsection (i) is replaced with:

"the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";

m. Clause 17 is replaced with:

"These Clauses are governed by the laws of England and Wales.";

n. Clause 18 is replaced with:

"Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."; and

o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

AMENDMENTS TO THIS ADDENDUM

16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.

17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

18. From time to time, the ICO may issue a revised Approved Addendum which:

    a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or
    b. reflects changes to UK Data Protection Laws;

    The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 "Ending the Addendum when the Approved Addendum changes", will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:

    a its direct costs of performing its obligations under the Addendum; and/or

b its risk under the Addendum,

and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

20. The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.

Alternative Part 2 Mandatory Clauses:

Mandatory Clauses	Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.