Date: 5th November 2024

A Contract for Services

Between

The Secretary of State for Justice

And

Redline Aviation Security Limited

Contents

A GENERAL 4

A1 DEFINITIONS AND INTERPRETATION 4
A2 AUTHORITY OBLIGATIONS 21
A3 SUPPLIER'S STATUS 22
A4 MISTAKES IN INFORMATION 22
A5 TERM 22

B THE SERVICES 22

B1 BASIS OF THE CONTRACT 22
B2 DELIVERY OF THE SERVICES 22
B3 EQUIPMENT 24
B4 KEY PERSONNEL 25
B5 STAFF 25
B6 DUE DILIGENCE 26
B7 LICENCE TO OCCUPY 26
B8 PROPERTY 27
B9 OFFERS OF EMPLOYMENT 27
B10 EMPLOYMENT 28
B11 IMPLEMENTATION 30

C PAYMENT 30

C1 PAYMENT AND VAT 30
C2 RECOVERY OF SUMS DUE 33
C3 PRICE DURING EXTENSION 34

D PROTECTION OF INFORMATION 34

D1 AUTHORITY DATA 34
D2 DATA PROTECTION AND PRIVACY 35
D3 OFFICIAL SECRETS ACTS AND FINANCE ACT 39
D4 CONFIDENTIAL INFORMATION 40
D5 FREEDOM OF INFORMATION 42
D6 PUBLICITY, MEDIA AND OFFICIAL ENQUIRIES 42

E INTELLECTUAL PROPERTY 43

E1 INTELLECTUAL PROPERTY RIGHTS 43

F CONTROL OF THE CONTRACT 45

F1 CONTRACT PERFORMANCE 45
F2 REMEDIES 46
F3 TRANSFER AND SUB-CONTRACTING 47
F4 CHANGE 50
F5 AUDIT 51

G LIABILITIES 53

G1 LIABILITY, INDEMNITY AND INSURANCE 53
G2 WARRANTIES AND REPRESENTATIONS 55
G3 TAX COMPLIANCE 56

H DEFAULT, DISRUPTION AND TERMINATION 56

H1 INSOLVENCY AND CHANGE OF CONTROL 57
H2 DEFAULT 59
H3 TERMINATION ON NOTICE 60
H4 OTHER GROUNDS 60

H5 CONSEQUENCES OF EXPIRY OR TERMINATION 60
H6 DISRUPTION 61
H7 RECOVERY 61
H8 RETENDERING AND HANDOVER 62
H9 EXIT MANAGEMENT 63
H10 KNOWLEDGE RETENTION 63
H11 BUSINESS CONTINUITY AND DISASTER 64

GENERAL 64

I1 DISPUTE RESOLUTION 64
I2 FORCE MAJEURE 66
I3 NOTICES AND COMMUNICATIONS 67
I4 CONFLICTS OF INTEREST 68
I5 RIGHTS OF THIRD PARTIES 68
I6 REMEDIES CUMULATIVE 69
I7 WAIVER 69
I8 SEVERABILITY 69
I9 ENTIRE AGREEMENT 69
I10 CHANGE IN LAW 70
I11 COUNTERPARTS 70
I12 GOVERNING LAW AND JURISDICTION 70

EXECUTION 123

Schedules

SCHEDULE 1 – SPECIFICATION 72

ANNEX 1: HMCTS SITES 72

ANNEX 2: SSOPS 72

SCHEDULE 2 – PRICES AND INVOICING 73

SCHEDULE 3 - CHANGE CONTROL 73

SCHEDULE 4 - COMMERCIALLY SENSITIVE INFORMATION 75

SCHEDULE 5 - SUPPLIER AND THIRD PARTY SOFTWARE 76

SCHEDULE 6 – INFORMATION SECURITY AND ASSURANCE 77

ANNEX 1: SECURITY REQUIREMENTS 86

ANNEX 2: SECURITY REQUIREMENTS FOR SUB-CONTRACTORS 93

ANNEX 3: SECURITY MANAGEMENT PLAN TEMPLATE 97

SCHEDULE 7 - PRISONS 103

SCHEDULE 8 – STATUTORY OBLIGATIONS AND CORPORATE SOCIAL RESPONSIBILITY ... 105

SCHEDULE 9 – DATA PROCESSING 111

SCHEDULE 10 – IMPLEMENTATION PLAN 113

SCHEDULE 11 – BUSINESS CONTINUITY AND DISASTER RECOVERY 116

SCHEDULE 12 – EXIT MANAGEMENT 121

This Contract is dated: 05/11/24

PARTIES:

(1) THE SECRETARY OF STATE FOR JUSTICE of 102 Petty France, London, SW1H 9AJ acting as part of the Crown (the "**Authority**");

AND

(2) Redline Aviation Security Limited with registered company number 05915087 whose registered office is c/o Air Partner, 2 City Place, Beehive Ring Road, Gatwick, West Sussex, RH6 0PA (the "**Supplier**")

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

WHEREAS

A. Following a competitive tender process, the Authority wishes to appoint the Supplier to provide the Services and the Supplier agrees to provide the Services in accordance with these terms and conditions.

NOW IT IS HEREBY AGREED:

A GENERAL

A1 Definitions and Interpretation

Unless the context otherwise requires the following terms shall have the meanings given to them below:

"**Abortive Test"** means a Covert Test that cannot be carried out as planned due to the fault of the Supplier or Staff including, without limitation, where the Tester is identified, the Prohibited Item is not in the correct position or there is too much clutter in the Tester's bag.

"**Ad Hoc Projects**" means any requirement for the Supplier to either (i) deliver more bespoke covert testing at high profile sites, or with new emerging threats, at HMCTS Sites and head office buildings across the Authority Premises, (ii) compliance-based access control and perimeter security control covert testing at Authority Premises, (iii) Penetration Testing or Improvised Explosive Device Testing at Authority Premises, or (iv) any security training/guidance focused on security search on entry skills and general security standards for

court security officers and the Senior Person on Site at Authority Premises, as may be requested from time to time by the Authority submitting a RFQ to the Supplier.

"**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.

"**Anti-Malicious Software**" means software which scans for and identifies possible Malicious Software in the ICT Environment.

"**Approve**", "**Approval**" and "**Approved**" means the prior written consent of the Authority.

"**Assessment Report**" means the report prepared by Supplier and accessible on the Secure Cloud-Based Reporting System within twenty-four (24) hours of a Covert Test taking place as part of the Core Services and as further described in Schedule 1.

"**Assessment Tool**" means the modern slavery risk identification and management tool which can be found at:

https://supplierregistration.cabinetoffice.gov.uk/msat

"**Associated Person**" means as it is defined in section 44(4) of the Criminal Finances Act 2017.

"**Authorised Representative**" means the Authority representative named in a CCN who is authorised to approve Changes.

"**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 (ii) which the Supplier is required to generate, process, store or transmit pursuant to the Contract; or

(b) any Personal Data for which the Authority is the Controller.

"**Authority Premises**" means any premises owned, occupied or controlled by the Authority or any other Crown Body which are made available for use by the Supplier or its Sub-Contractors for provision of the Services and includes HMCTS Sites.

"**Authority Software**" means software which is owned by or licensed to the Authority (other than under or pursuant to the Contract) and which is or will be used by the Supplier for the purposes of providing the Services.

"**Authority System**" means the Authority's computing environment (consisting of hardware, software and/or telecommunications networks or equipment) used by the Authority or the Supplier in connection with the Contract which is owned by or licensed to the Authority by a third party and which interfaces with the Supplier System or which is necessary for the Authority to receive the Services.

"**Authority Technical Security Guidance**" means the technical security guidance published by the Authority at:

https://security-guidance.service.justice.gov.uk/#cyber-and-technical-security-guidance

"**Basware**" means Basware eMarketplace, the procurement software used by the Authority for its financial transactions.
"**BPSS**" means the Government's Baseline Personnel Security Standard for Government employees.

"**Breach of Security**" means an event which results in or could result in:

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

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

"**BS 8555**" means the standard published to help organisations improve their environmental performance by the British Standards Institution.

"Business Continuity Disaster Recovery Plan" means the plan provided and containing the required information as set out in Schedule 11;

"**CCN**" means a contract change notice in the form set out in Schedule 3.

"**Certification Requirements**" means the requirements set out in paragraph 6 of Schedule 6.

"**Change**" means a change in any of the terms or conditions of the Contract.

"**Change Control Procedure**" means the procedure for changing this Contract set out in clause F4 (Change).

"**Change in Law**" means any change in Law which affects the performance of the Services which comes into force after the Commencement Date.

"**CHECK Service Provider**" means an organisation which has been certified by the NCSC, holds "Green Light" status and is authorised to provide the IT Health Check services required by paragraph 7.1 of Schedule 6.

"Cluster Manager" means the person responsible for operational delivery of a category of court or category of court activity within a location or jurisdiction for the Authority.

"**Commencement Date**" means the date specified in clause A5.1.

"**Commercially Sensitive Information**" means the information listed in Schedule 4 comprising the information of a commercially sensitive nature relating to:

(a) the Price; and/or

(b) the Supplier's business and investment plans

which the Supplier has informed the Authority would cause the Supplier significant commercial disadvantage or material financial loss if it was disclosed.

"**Comparable Supply**" means the supply of services to another customer of the Supplier which are the same or similar to any of the Services.

"**Confidential Information**" means any information which has been designated as confidential by either Party in writing or that ought to be considered as confidential (however it is conveyed or on whatever media it is stored) including information the disclosure of which would, or would be likely to, prejudice the commercial interests of any person or trade secrets or Intellectual Property Rights of either Party and all Personal Data. Confidential Information shall not include information which:

(a) was public knowledge at the time of disclosure otherwise than by breach of clause E4;

(b) was in the possession of the receiving Party, without restriction as to its disclosure, before receiving it from the disclosing Party;

(c) is received from a third party (who lawfully acquired it) without restriction as to its disclosure; or

(d) is independently developed without access to the Confidential Information.

"**Contract**" means these terms and conditions, the attached Schedules and any other provisions the Parties expressly agree are included.

"**Contracting Authority**" means any contracting authority (other than the Authority) as defined in regulation 2 of the Regulations.

"**Contracts Finder**" means the Government's portal for public sector procurement opportunities.

"**Control**" means that a person possesses, directly or indirectly, 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**" are interpreted accordingly.

"**Controller**" means as it is defined in the UK GDPR.

"**Copyright**" means as it is defined in s.1 of Part 1 Chapter 1 of the Copyright, Designs and Patents Act 1988.

"**Core Requirement Pricing**" means the Supplier's pricing submitted as part of the Tender to cover the Core Services.

"**Core Services**" has the meaning set out in Schedule 1 of this Contract.

"**CREST Service Provider**" means an organisation with a SOC Accreditation from CREST International.

"**Crown**" means the government of the UK (including the Northern Ireland Executive Committee and Northern Ireland Departments, the Scottish Executive and the National Assembly for Wales), including, but not limited to, Government ministers, Government

departments, Government offices and Government agencies and "**Crown Body**" is an emanation of the foregoing.

"**Counter Terrorist Check (CTC) Clearance**" means one of the five main levels of national security clearance whose checks will involve:

- successful completion of the baseline personnel security standard
- completion, by the individual, of a security questionnaire
- a departmental/company records check which might include, for example personal files, staff reports, sick leave returns and security records
- a check of both spent and unspent criminal records
- a check of Security Service (MI5) records, and
- if there are any unresolved security concerns about the individual or if recommended by the Security Service, the individual may also be interviewed.

"Covert Test" means an authorised attempt by a Tester as part of the Services to access any Authority Premises in order to test the effectiveness of the Security Services Provider's search on entry 'security screening' procedures.

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

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

"**Cyber Essentials Scheme**" means the Cyber Essentials scheme operated by the NCSC.

"**Data Loss Event**" means any event which results, or may result, in unauthorised access to Personal Data held by the Supplier under the Contract, and/or actual or potential loss and/or destruction of Personal Data in breach of the Contract, including any Personal Data breach.

"**Data Protection Law**" means:

(a) all applicable UK Law relating to the processing of Personal Data and privacy; including the UK GDPR and the DPA to the extent it relates to Processing of Personal Data and privacy; and

(b) (to the extent that it applies) the EU GDPR.

"**Data Protection Officer**" means as it is defined in the UK GDPR.

"**Data Subject**" means as it is defined in the UK GDPR.

"**Data Subject Request**" means a request made by or on behalf of a Data Subject in accordance with rights granted pursuant to Data Protection Law to access their Personal Data.

"**Database Rights**" means as rights in databases are defined in s.3A of Part 1 Chapter 1 of the Copyright, Designs and Patents Act 1988.

"**Default**" means any breach of the obligations or warranties of the relevant Party (including abandonment of the Contract in breach of its terms, repudiatory breach or breach of a fundamental term) or any other default, act, omission, negligence or statement of the relevant Party or the Staff in connection with the subject-matter of the Contract and in respect of which such Party is liable to the other.

"**Delay**" means a delay in the:

(a) achievement of a Milestone by its Milestone Date; or

(b) 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 Contract set out in the Implementation Plan.

"Disaster" means the occurrence of one or more events which, either separately or cumulatively, mean that the Services, or a material part thereof will be unavailable (or could reasonably be anticipated to be unavailable).

"Dispute Resolution Procedure" means as it is defined in I1.

"**DOTAS**" means the Disclosure of Tax Avoidance Schemes rules which require a promotor 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 and as extended to NICs by the National Insurance (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.

"**DPIA**" means a data protection impact assessment by the Controller carried out in accordance with s.3 of the UK GDPR and s.64 and s.65 of the DPA.

"**EEA**" means the European Economic Area.

"**EIR**" means the Environmental Information Regulations 2004 (SI 2004/3391) and any guidance and/or codes of practice issued by the ICO or relevant Government department in relation to such regulations.

"Employees" means those persons agreed by the Parties to be employed by the Supplier (and/or any Sub-Contractor) wholly or mainly in the supply of the Services immediately before the end of the Term.

"**End Date**" means the date specified in clause A5.1.

"**Equipment**" means the Supplier's equipment, consumables, plant, materials and such other items supplied and used by the Supplier in the delivery of the Services.

"**EU**" means the European Union.

"**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 on the free movement of Personal Data (General Data Protection Regulation) as it has effect in EU law.

"**Exit Day**" means as it is defined in the Withdrawal Act.

"**Extension**" means as it is defined in clause A5.2.

"Facilities Manager" means the individual who manages all property and Facilities Management (FM) related activities at site level for the Authority.

"**Financial Year**" means the period from 1st April each year to the 31st March the following year.

"**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 ICO in relation to such legislation.

"**Force Majeure Event**" means any event outside the reasonable control of either Party affecting its performance of its obligations under the Contract 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, for flood, storm or earthquake, or disaster but excluding any industrial dispute relating to the Supplier or the Staff or any other failure in the Supplier's supply chain caused by the Covid 19 pandemic or the UK's exit from the EU.

"**General Anti-Abuse 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 NICs.

"**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 standards, practices, methods and procedures conforming to the Law and the degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person or body engaged in a similar type of undertaking under the same or similar circumstances.

"**Government**" means the government of the UK.

"**Government Buying Standards**" means the standards published here:

https://www.gov.uk/government/collections/sustainable-procurement-the-government-buying-standards-gbs

"**Greening Government Commitments**" means the Government's policy to reduce its effects on the environment, the details of which are published here:

https://www.gov.uk/government/collections/greening-government-commitments

"**Halifax Abuse Principle**" means the principle explained in the CJEU Case C-255/02 Halifax and others.

"**Head of Regional Support Unit**" means the individual who supports the delivery director and the regional security and safety champion to fulfil their security and safety obligations for the Authority.

"**Higher Risk Sub-contractor**" means a Sub-Contractor which processes Authority Data where that data includes:

(a) the Personal Data of 1000 or more individuals in aggregate during the Term; or
(b) any part of that data includes any of the following:

i) financial information relating to any person;
ii) any information relating to actual or alleged criminal offences;
iii) any information relating to vulnerable people;
iv) any information relating to social care;
v) any information relating to a person's employment;
vi) Special Category Personal Data;

(c) the Authority, at its discretion designates a Sub-Contractor as a Higher Risk Sub-contractor in any procurement document related to the Contract; or

(d) the Authority considers, at its discretion, that any actual or potential Processing carried out by the Sub-Contractor is high risk.

"HMCTS" means HM Courts and Tribunals Service, an executive agency responsible for the administration of criminal, civil and family courts and tribunals in England and Wales, sponsored by the Authority.

"HMCTS Head of Security and Safety" means the individual who leads on the development and maintenance of health and safety, security and fire safety policies for HMCTS

"**HMCTS Regions**" means [the seven (7) geographical areas covered under the Contract. They are London, South East, South West, Midlands, Wales, North West and North East & Scotland.

"**HMCTS Security Contract Lead"** means the individual who leads on the operational performance management of the Contract for the Authority.

"**HMCTS Sites**" means the list of courts and tribunals that currently make up the HMCTS estate as set out in Annex 1 of Schedule 1, as such list may be updated from time to time by the Authority and notified to the Supplier.

"**HMRC**" means HM Revenue & Customs.

"**ICO**" means the Information Commissioner's Office.

"**ICT Environment**" means the Authority System and the Supplier System.

"**Improvised Explosive Device Testing**" or "**IED Testing**" means a Covert Test safely delivered as part of an Ad Hoc Project to verify that Improvised Explosive Device (s), or an IED component part as defined in the SSOPs, are not present on the Tester or in the Tester's bags.

"**Implementation Plan**" means the Implementation Plan as further detailed in Schedule 10 of this Contract as updated as agreed between Supplier and the Authority from time to time.

"**Incident Management Process**" means the process which the Supplier shall implement immediately after it becomes aware of a Breach of Security which is intended to restore normal operations as quickly as possible, minimising any adverse effect on the Authority Data, the Authority, the Services and/or users of the Services and which shall be shall be prepared by the Supplier in accordance with paragraph 4Information Security Approval Statement of Schedule 6 using the template set out in annex 3 of Schedule 6.

"**Information**" has the meaning given under section 84 of the FOIA.

"**Information Assets**" means definable pieces of information stored in any manner which are determined by the Authority to be valuable and relevant to the Services.

"**Information Assurance Assessment**" means the set of policies, procedures, systems and processes which the Supplier shall implement, maintain and update in accordance with paragraph 4 of Schedule 6 in order to manage, mitigate and, where possible, avoid information security risks including cyber-attacks, hacks, data leaks, Personal Data Breaches and/or theft and which shall be prepared by the Supplier using the template set out in **Error! Reference source not found.** of Schedule 6.

"**Information Management System**" means:

(a) those parts of the Supplier System, and those of the Premises, which the Supplier or its Sub-contractors use to provide the parts of the Service which require Processing Authority Data; and

(b) the associated information assets and systems (including organisational structure, controls, policies, practices, procedures, processes and resources).

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

(a) the Authority is satisfied that the identified risks have been adequately and appropriately addressed;

(b) the Authority has accepted the residual risks; and

(c) the Supplier may use the Information Management System to process Authority Data.

"**Initial Term**" means the period from the Commencement Date to the End Date.

"**Intellectual Property Rights**" means:

(a) patents, utility models, inventions, trademarks, service marks, logos, design rights (whether registrable or otherwise), Database Rights, domain names, semi-conductor topography rights, rights in Internet domain names, Know-How, trade or business names, moral rights, the right to sue for passing off, trade secrets and other rights in Confidential Information, in each whether registrable or not in any country;

(b) applications for registration, and the right to apply for registration, for any of the rights listed in (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.

"**ISO**" means the International Organisation for Standardisation.

"**ISO/IEC 14001**" means the family of standards related to environmental management published by the ISO.

"**ISO/IEC 27001**" means the family of standards related to information security management published by the ISO.

"**ISO/IEC 27002**" means the family of standards related to information security, cyber security and privacy protection published by the ISO.

"**ITEPA**" means the Income Tax (Earnings and Pensions) Act 2003.

"**IT Health Check**" means as it is defined in paragraph 7.1(a) of Schedule 6.

"**Joint Controllers**" means as it is defined in Article 26 of the UK GDPR.

"**Key Milestones**" means the Milestones identified in the Implementation Plan as key milestones and in respect of which the Authority could Delay Payments if the key milestones are not met by the relevant Milestone Date

"**Key Personnel**" mean the people named in the Specification as key personnel, if any.

"**Knife Test"** means an attempt by an anonymous Tester to covertly bring in a 3" optimal knife Test Piece to any Authority Premises.

"**Know-How**" means all information not in the public domain held in any form (including without limitation that comprised in or derived from drawings, data formulae, patterns, specifications, notes, samples, chemical compounds, biological materials, computer software, component lists, instructions, manuals, brochures, catalogues and process descriptions and scientific approaches and methods).

"**Law**" means any law, statute, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements with which the Supplier is bound to comply.

"**Law Enforcement Purposes**" means as it is defined in the DPA.

"**LED**" means the Law Enforcement Directive (Directive (EU) 2016/680).

"**Losses**" means losses, liabilities, damages, costs, fines 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.

"**Material Breach**" means a breach (including an anticipatory breach):

(a) which has a material effect on the benefit which the Authority would otherwise derive from a substantial or material portion of the Contract; or

(b) of any of the obligations set out in clauses B11.3(d), D1, D2, D3, D4, G3, I4 or paragraph 9 of Schedule 8.

"**Medium Risk Sub-contractor**" means a Sub-Contractor which processes Authority Data where that data:

(a) includes the Personal Data of between 100 and 999 individuals (inclusive) in aggregate during the Term; and

(b) does not include Special Category Personal Data.

"**Milestone**" means an event or task described in the Implementation Plan which, if applicable, shall be completed by the relevant Milestone Date.

"**Milestone Date**" means the target date set out against the relevant Milestone in the Implementation Plan by which the Milestone must be achieved.

"Mobilisation Period" means a period of three (3) Months beginning on the Commencement Date.

"**Modern Slavery Helpline**" means the point of contact for reporting suspicion, seeking help or advice and information on the subject of modern slavery available by telephone on 08000 121 700 or online at:

https://www.modernslaveryhelpline.org/report

"**Month**" means calendar month.

"**MSA**" means the Modern Slavery Act 2015.

"**National Security Vetting**" means checks carried out by UK Security Vetting (UKSV) to provide a level of assurance as to the trustworthiness, integrity, reliability and resilience of an individual to handle sensitive information or assets as currently set out in SSOP 40 - FM Suppliers and Security Suppliers Staff Security Requirements and as may be updated from time to time by the Authority and notified to the Supplier.

"**NCSC**" means the National Cyber Security Centre.

"**NICs**" means National Insurance Contributions.

"**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 which 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 the 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 Commencement Date or to a civil penalty for fraud or evasion.

"**Open Book Data**" means complete and accurate financial and non-financial information which is sufficient to enable the Authority to verify:

(a) the Price already paid or payable and the Price forecast to be paid during the remainder of the Term;

(b) the Supplier's costs and manpower resources broken down against each element of the Services;

(c) the cost to the Supplier of engaging the Staff, including base salary, tax and pension contributions and other contractual employment benefits;

(d) operational costs which are not included within the above, to the extent that such costs are necessary and properly incurred by the Service Provider in the delivery of the Services;

(e) all interest, expenses and any other third party financing costs incurred in relation to the provision of the Services; and

(f) the profit achieved over the Term and annually.

"Penetration Testing" means a security exercise where a Tester attempts to find and exploit vulnerabilities in the execution of a security standard policy such as search on entry procedures or access control arrangements.

"**Personal Data**" means as it is defined in the UK GDPR.

"**Personal Data Breach**" means as it is defined in the UK GDPR.

"**Premises**" means the location where the Services are to be supplied set out in the Specification.

"**Price**" means the price (excluding any applicable VAT) payable to the Supplier by the Authority under the Contract, as set out in Schedule 2 for the full and proper performance by the Supplier of its obligations under the Contract.

"**Processing**" means as it is defined in Article 4 of the UK GDPR and "**Process**" is construed accordingly.

"**Processor**" means as it is defined in the UK GDPR.

"**Prohibited Act**" means:

(a) to directly or indirectly offer, promise or give any person working for or engaged by the Authority 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 the Contract;

(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) the defrauding, attempting to defraud or conspiring to defraud the Authority;

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

"**Prohibited Item**" means an item not permitted to be brought into any Authority Premises as currently set out in Schedule 1 (Specification), Annex 2, SSOP 4e, as may be updated from time to time.

"Prohibited Item Test" means an attempt by a Tester to covertly bring in a small Prohibited Item either on the Tester's person or in the Tester's bags into any Authority Premises.

"**Property**" means the property, other than real property, made available to the Supplier by the Authority in connection with the Contract.

"**Protective Measures**" means appropriate technical and organisational measures designed to ensure compliance with obligations of the Parties arising under Data Protection Law and the Contract which may include: pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the measures adopted.

"**PSI 07/2016**" is the Prison Service Instruction published on 26th October 2016 relating to the searching of the person as amended from time to time and available at:

https://www.gov.uk/government/publications/procedures-for-searching-people-psi-072016

"**PSI 10/2012**" is the Prison Service Instruction published on 26 March 2012 relating to the Conveyance and Possession of Prohibited Items and other Related Offences as amended from time to time and available at:

https://www.gov.uk/government/publications/controlling-banned-prohibited-items-psi-102012

"**PSI 07/2014**" is the Prison Service Instruction published on 2nd June 2014 relating to security vetting as amended from time to time and available at:

https://www.gov.uk/government/publications/security-vetting-psi-072014-pi-032014

"**Purchase Order**" the Authority's order for the supply of the Services.

"**Quality Standards**" means the quality standards published by BSI British Standards, the National Standards Body of the UK, the International Organisation for Standardization or other reputable or equivalent body (and their successor bodies) that a skilled and experienced operator in the same type of industry or business sector as the Supplier would reasonably and ordinarily be expected to comply with, and as may be further detailed in Schedule 1.

"Regional Facilities Manager" means the individual who manages all property and Facilities Management (FM) related activities across one of seven HMCTS Regions.

"Regional Security and Safety Officer" means the individual who supports the regional security and safety champion and the regional support unit to maintain good security and safety practice and legal compliance across the region.

"**Regulations**" means the Public Contracts Regulations 2015 (SI 2015/102).

"**Regulator Correspondence**" means any correspondence from the ICO or any successor body in relation to the processing of Personal Data under the Contract.

"**Regulatory Body**" means a Government department and regulatory, statutory and other entities, committees, ombudsmen and bodies which, whether under statute, rules, regulations, codes of practice or otherwise, are entitled to regulate, investigate, or influence the matters dealt with in the Contract or any other affairs of the Authority.

"**Related Supplier**" means (a) any person who provides services to the Authority which is related to the Services from time to timed/or (b) any providers of other services, works or supplies to the Authority's Premises.

"**Relevant Conviction**" means a conviction that is relevant to the nature of the Services or as listed by the Authority and/or relevant to the work of the Authority.

"**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.

"**Remediation Plan**" means as it is defined in paragraph 7.3(c)(i) of Schedule 6.

"**Replacement Supplier**" means any third-party supplier appointed by the Authority to supply any services which are substantially similar to any of the Services in substitution for any of the Services following the expiry, termination or partial termination of the Contract.

"**Request for Information**" means a request for information under the FOIA or the EIR.

"**Required Changes Register**" means the register within the Security Management Plan which is to be maintained and updated by the Supplier and which shall record each of the changes that the Supplier shall make to the Information Management System and/or the Security Management Plan as a consequence of the occurrence of any of the events set out in paragraph 5.2 of Schedule 6 together with the date by which such change shall be implemented and the date on which such change was implemented.

"**Results**" means any guidance, specifications, reports, studies, instructions, toolkits, plans, data, drawings, databases, patents, patterns, models, designs or other material which is:

a) prepared by or for the Supplier for use in relation to the performance of its obligations under the Contract; and/or

b) the result of any work done by the Supplier or any Staff in relation to the provision of the Services.

"**RFQ**" means a request for quotation issued by the Authority to the Supplier for Ad Hoc Projects from time to time.

"**Risk Register**" means the risk register within the Information Assurance Assessment which is to be prepared and submitted for Approval in accordance with paragraph 4 of Schedule 6.

"**Secure Cloud-Based Reporting System**" means the Supplier's cloud-based reporting system that is accessible from a government secure network and is capable of providing downloadable reports of the information detailed in Schedule 1.

"Security and Safety Operating Procedure (SSOP)" means the documents that set out the standards and mandatory requirements that must be observed by Security Services Providers in order to protect the Authority from security threats as included at Annex 2 of Schedule 1 and as may be updated from time to time.

"Security Check (SC)" means a national security clearance level required–by SSOP 40 - FM Suppliers and Security Suppliers Staff Security Requirements as may be updated from time by the Authority and notified to the Supplier.

"**Security Incident**" means the access to the ICT Environment by an unauthorised person for any reason or the unauthorised alteration of the functionality of the ICT Environment.

"**Security Management Plan**" means the plan prepared by the Supplier using the template in Annex 3 of Schedule 6, comprising:

(a) the Information Assurance Assessment;
(b) the Required Changes Register; and
(c) the Incident Management Process.

"**Security Policy Framework**" means the Government's security policy framework (available from the Cabinet Office's Government Security Secretariat) as updated from time to time.

"**Security Services Provider**" means the contracted organisation that provides the court security officers to the relevant Authority Premises.

"**Senior Person on Site**" means the person(s) identified by the Authority in writing from time to time as the person(s) at each of the Authority Premises who is responsible for the overall security and safety of the relevant Authority Premises.

"**Service Delivery Start Date**" means the next calendar day which immediately follows the end of the Mobilisation Period

"**Services**" means the services set out in Schedule 1 (including any modified or alternative services) and includes the Core Services and Ad Hoc Projects.

"Sip Test" means a test to verify that any drink carried on a Tester or in the Tester's bags when they seek to gain access to any Authority Premises contains water or a soft drink and not a poisonous or otherwise dangerous liquid, achieved by the on-duty security officer requiring the Tester to sip the contents of the drink in its container.

"**SME**" means an enterprise falling within the category of micro, small and medium-sized enterprises defined by the European Commission's Recommendation of 6 May 2003 available at:

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2003:124:0036:0041:en:PDF

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

"**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.

"**Specification**" means the description of the Services to be supplied under the Contract as set out in Schedule 1 including, where appropriate, the Key Personnel, the Premises and the Quality Standards.

"**SSCBA**" means the Social Security Contributions and Benefits Act 1992.

"**Staff**" means all directors, officers, employees, agents, consultants and contractors of the Supplier and/or of any of its Sub-Contractors engaged in the performance of the Supplier's obligations under the Contract, including any Testers.

"**Sub–Contract**" means a contract between two or more suppliers, at any stage of remoteness from the Authority in a sub-contracting chain, made wholly or substantially for the purpose of performing (or contributing to the performance of) the whole or any part of the Contract and "**Sub-Contractor**" shall be construed accordingly.

"**Sub-processor**" means any third party appointed to process Personal Data on behalf of the Supplier related to the Contract.

"Supplier Operating Procedure" means the Supplier document that sets out the Supplier's standards and mandatory procedures for delivering the Services.

"**Supplier Software**" means software which is proprietary to the Supplier, including software which is or will be used by the Supplier for the purposes of providing the Services and which is set out in Schedule 5.

"**Supplier System**" means the information and communications technology system used by the Supplier in performing the Services including the Secure Cloud-Based Reporting System, the Supplier Software, the Equipment and related cabling (but excluding the Authority System).

"**Tender**" means the Supplier's tender submitted in response to the Authority's invitation to suppliers for offers to supply the Services.

"**Term**" means the period from the Commencement Date to:

(a) the End Date; or

(b) following an Extension, the end date of the Extension

or such earlier date of termination or partial termination of the Contract in accordance with the Law or the Contract.

"Tester" means a security professional accredited and security cleared to undertake a Covert Test.

"**Test Piece**" means a physical item which imitates a Prohibited Item and is agreed between the Authority and the Supplier as part of the Services.

"**Third Party IP Claim**" has the meaning given to it in clause E1.5.

"**Third Party Software**" means software which is proprietary to any third party which is or will be used by the Supplier to provide the Services including the software and which is specified as such in Schedule 5.

"**TUPE**" means the Transfer of Undertakings (Protection of Employment) Regulations 2006.

"**TUPE Information**" means the information set out in clause B10.1.

"**UK**" means United Kingdom.

"**UK GDPR**" means the UK General Data Protection Regulation.

"**Valid Invoice**" means an invoice containing the information set out in clause C1.3 or C1.4.

"**VAT**" means value added tax charged or regulated in accordance with the Value-Added Tax Act 1994.

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

"**Welsh Language Scheme**" means the Authority's Welsh language scheme as amended from time to time and available at:

http://www.justice.gov.uk/publications/corporate-reports/moj/2010/welsh-language-scheme

"**Withdrawal Act**" means the European Union (Withdrawal) Act 2018.

"**Working Day**" means a day (other than a Saturday or Sunday) on which banks are open for general business in the City of London.

In the Contract, unless the context implies otherwise:

(a) the singular includes the plural and vice versa unless the context requires otherwise;

(b) words importing the masculine include the feminine and the neuter;

(c) reference to a clause is a reference to the whole of that clause unless stated otherwise;

(d) references to a person include natural persons, a company, body corporate, corporation, unincorporated association, firm, partnership or other legal entity or central Government body;

(e) the words "other", "in particular", "for example", "including" 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";

(f) headings are included for ease of reference only and shall not affect the interpretation or construction of the Contract;

(g) the annexes and Schedules form an integral part of the Contract and have effect as if set out in full in the body of the Contract. A reference to the Contract includes the annexes and Schedules;

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

(i) references to the Contract are references to the Contract as amended from time to time; and

(j) any reference in the Contract which immediately before Exit Day was a reference to (as it has effect from time to time):

(i) 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 Withdrawal Act shall be read as a reference to the EU References as they form part of domestic law by virtue of section 3 of the Withdrawal Act as modified by domestic law from time to time; and

(ii) any EU institution or EU authority or other such EU body shall be read as a reference to the UK institution, authority or body to which its functions were transferred.

A2 Authority Obligations

Save as otherwise expressly provided, the Authority's obligations under the Contract are the Authority's obligations in its capacity as a contracting counterparty and nothing

in the Contract operates as an obligation upon, or in any other way fetters or constrains, the Authority in any other capacity.

A3 Supplier's Status

A3.1 The Supplier is an independent contractor and nothing in the Contract creates a contract of employment, a relationship of agency or partnership or a joint venture between the Parties and accordingly neither Party is authorised to act in the name of, or on behalf of, or otherwise bind the other Party save as expressly permitted by the Contract.

A3.2 The Supplier shall not (and shall ensure that any other person engaged in relation to the Contract shall not) say or do anything that might lead another person to believe that the Supplier is acting as the agent or employee of the Authority.

A4 Mistakes in Information

The Supplier is responsible for the accuracy of all drawings, documentation and information supplied to the Authority by the Supplier in connection with the Services and shall pay the Authority any extra costs occasioned by any discrepancies, errors or omissions therein.

A5 Term

A5.1 The Contract starts on 1st November 2024 (the "**Commencement Date**") and ends on 31st October 2026 (the "**End Date**") unless it is terminated early or extended in accordance with the Contract.

A5.2 The Authority may extend the term of the Contract ("**Extension**") up to a maximum of four years. The terms of the Contract will apply throughout the period of any Extension.

B THE SERVICES

B1 Basis of the Contract

B1.1 In consideration of the Supplier's performance of its obligations under the Contract the Authority shall pay the Supplier the Price in accordance with clause C1.

B1.2 The terms and conditions in the Contract apply to the exclusion of any other terms and conditions the Supplier seeks to impose or incorporate, or which are implied by trade, custom, practice or course of dealing.

B2 Delivery of the Services

B2.1 The Supplier shall at all times comply with the Quality Standards and, where applicable, shall maintain accreditation with the relevant Quality Standards authorisation body. To the extent that the standard of the Service has not been specified in the Contract, the Supplier shall agree the relevant standard of the Services with the Authority prior to the supply of the Services and, in any event, the Supplier shall perform its obligations under the Contract in accordance with the Law and Good Industry Practice.

B2.2 The Supplier acknowledges that the Authority relies on the skill and judgment of the Supplier in the supply of the Services and the performance of the Supplier's obligations under the Contract.

B2.3 The Supplier shall:

(a) ensure that all Staff supplying the Services do so with all due skill, care and diligence and shall possess such qualifications, skills and experience as are necessary for the proper supply of the Services;

(b) ensure that all Staff are properly managed and supervised; and

(c) comply with the standards and requirements set out in the Specification and Schedule 8.

B2.4 If the Specification includes installation of equipment the Supplier shall notify the Authority in writing when it has completed installation. Following receipt of such notice, the Authority shall inspect the installation and shall, by giving notice to the Supplier:

(a) accept the installation; or

(b) reject the installation and inform the Supplier why, in the Authority's reasonable opinion, the installation does not satisfy the Specification.

B2.5 If the Authority rejects the installation pursuant to clause B2.4 (b), the Supplier shall immediately rectify or remedy any defects and if, in the Authority's reasonable opinion, the installation does not, within 2 Working Days or such other period agreed by the Parties, comply with the Specification, the Authority may terminate the Contract with immediate effect.

B2.6 The installation is complete when the Supplier receives a notice issued by the Authority in accordance with clause B2.4 (a). Notwithstanding acceptance of any installation in accordance with clause B2.4 (a), the Supplier is solely responsible for ensuring that the Services and the installation conform to the Specification. No rights of estoppel or waiver shall arise as a result of the acceptance by the Authority of the installation.

B2.7 During the Term, the Supplier shall:

(a) at all times have all licences, approvals and consents necessary to enable the Supplier and Staff to carry out the installation;

(b) provide all tools and equipment (or procure the provision of all tools and equipment) necessary for completion of the installation;

(c) not, in delivering the Services, in any manner endanger the safety or convenience of the public.

B2.8 The Authority may inspect the manner in which the Supplier supplies the Services at the Premises during normal business hours on reasonable notice. The Supplier shall provide at its own cost all such facilities as the Authority may reasonably require for such inspection. In this clause B2, Services include planning or preliminary work in connection with the supply of the Services.

B2.9 If reasonably requested to do so by the Authority, the Supplier shall co-ordinate its activities in supplying the Services with those of the Authority and other contractors engaged by the Authority.

B2.10 Timely supply of the Services is of the essence of the Contract, including in relation to commencing the supply of the Services within the time agreed or on a specified date. If the Supplier fails to supply the Services within the time promised or specified in the Specification, the Authority is released from any obligation to pay for the Services and may terminate the Contract, in either case without prejudice to any other rights and remedies of the Authority.

B2.11 If the Authority informs the Supplier in writing that the Authority reasonably believes that any part of the Services do not meet the requirements of the Contract or differs in any way from those requirements, and this is not as a result of a default by the Authority, the Supplier shall at its own expense re-schedule and carry out the Services in accordance with the requirements of the Contract within such reasonable time as may be specified by the Authority.

B2.12 If, in delivering the Services, the Supplier is required to visit Authority Premises which are prisons, the Supplier shall comply with Schedule 7.

B3 Equipment

B3.1 The Supplier shall provide all the Equipment and resource necessary for the supply of the Services.

B3.2 The Supplier shall not deliver any Equipment to, or begin any work on, the Premises without Approval.

B3.3 All Equipment brought onto the Premises is at the Supplier's own risk and the Authority has no liability for any loss of or damage to any Equipment unless the Supplier demonstrates that such loss or damage was caused or contributed to by the Authority's Default. The Supplier shall provide for the haulage or carriage thereof to the Premises and the removal of Equipment when no longer required at its sole cost.

B3.4 Equipment brought onto the Premises remains the property of the Supplier.

B3.5 If the Authority reimburses the cost of any Equipment to the Supplier the Equipment shall become the property of the Authority and shall on request be delivered to the Authority as directed by the Authority. The Supplier shall keep a full and accurate inventory of such Equipment and deliver that inventory to the Authority on request and on completion of the Services.

B3.6 The Supplier shall maintain all Equipment in a safe, serviceable and clean condition.

B3.7 The Supplier shall, at the Authority's written request, at its own cost and as soon as reasonably practicable:

(a) remove immediately from the Premises Equipment which is, in the Authority's opinion, hazardous, noxious or not supplied in accordance with the Contract; and

(b) replace such item with a suitable substitute item of Equipment.

B3.8 Within 20 Working Days of the end of the Term, the Supplier shall remove the Equipment together with any other materials used by the Supplier to supply the Services and shall leave the Premises in a clean, safe and tidy condition. The Supplier shall make good any damage to those Premises and any fixtures and fitting in the Premises which is caused by the Supplier or Staff.

B4 Key Personnel

B4.1 The Supplier acknowledges that Key Personnel are essential to the proper provision of the Services.

B4.2 Key Personnel shall not be released from supplying the Services without Approval except by reason of long-term sickness, maternity leave, paternity leave or termination of employment or other similar extenuating circumstances.

B4.3 The Authority may interview and assess any proposed replacement for Key Personnel and any replacements to Key Personnel are subject to Approval. Such replacements shall be of at least equal status, experience and skills to Key Personnel being replaced and be suitable for the responsibilities of that person in relation to the Services.

B4.4 The Authority shall not unreasonably withhold approval under clauses B4.2 or B4.3 and such approval is conditional on appropriate arrangements being made by the Supplier to minimise any adverse effect on the Services which could be caused by a change in Key Personnel.

B5 Staff

B5.1 The Authority may, by notice to the Supplier, refuse to admit onto, or withdraw permission to remain on, the Authority's Premises:

(a) any member of the Staff; or

(b) any person employed or engaged by any member of the Staff

whose admission or continued presence would, in the Authority's reasonable opinion, be undesirable.

B5.2 The Authority shall maintain the security of the Authority's Premises in accordance with its standard security requirements, including Prison Rules 1999 Part III, the Prison (Amendment) Rules 2005, the Young Offender Institute Rules 2000 Part III and the Young Offender Institute (Amendment) Rules 2008, available to the Supplier

on request. The Supplier shall comply with all security requirements of the Authority while on the Authority's Premises, and ensure that all Staff comply with such requirements.

B5.3 The Authority may search any persons or vehicles engaged or used by the Supplier at the Authority's Premises.

B5.4 At the Authority's written request, the Supplier shall, at its own cost, provide a list of the names, addresses, national insurance numbers and immigration status of all people who may require admission to the Authority's Premises, specifying the capacities in which they are concerned with the Contract and giving such other particulars as the Authority may reasonably request.

B5.5 The Supplier shall ensure that all Staff who have access to the Authority's Premises, the Authority System or the Authority Data have been cleared in accordance with the BPSS.

B5.6 The Supplier shall co-operate with any investigation relating to security carried out by the Authority or on behalf of the Authority and, at the Authority's request:

(a) use reasonable endeavours to make available any Staff requested by the Authority to attend an interview for the purpose of an investigation; and

(b) provide documents, records or other material in whatever form which the Authority may reasonably request or which may be requested on the Authority's behalf, for the purposes of an investigation.

B5.7 The Supplier shall comply with PSI 10/2012 as amended from time to time and available from the Authority on request.

B6 Due Diligence

Save as the Authority may otherwise direct, the Supplier is deemed to have inspected the Premises before submitting its Tender and to have completed due diligence in relation to all matters connected with the performance of its obligations under the Contract.

B7 Licence to Occupy

B7.1 Any land or Premises made available from time to time to the Supplier by the Authority in connection with the Contract are on a non-exclusive licence basis free of charge and are used by the Supplier solely for the purpose of performing its obligations under the Contract. The Supplier has the use of such land or Premises as licensee and shall vacate the same on termination of the Contract.

B7.2 The Supplier shall limit access to the land or Premises to such Staff as is necessary for it to perform its obligations under the Contract and the Supplier shall co-operate (and ensure that its Staff co-operate) with other persons working concurrently on such land or Premises as the Authority may reasonably request.

B7.3 If the Supplier requires modifications to the Authority's Premises such modifications are subject to Approval and shall be carried out by the Authority at the Supplier's cost.

B7.4 The Supplier shall (and shall ensure that any Staff on the Authority's Premises shall) observe and comply with such rules, regulations and requirements (including those relating to security arrangements) as may be in force from time to time for the conduct of personnel when on the Authority's Premises as determined by the Authority.

B7.5 The Contract does not create a tenancy of any nature in favour of the Supplier or its Staff and no such tenancy has or shall come into being and, notwithstanding any rights granted pursuant to the Contract, the Authority may use the Premises owned or occupied by it in any manner it sees fit.

B8 Property

B8.1 All Property is and remains the property of the Authority and the Supplier irrevocably licenses the Authority and its agents to enter any Premises of the Supplier during normal business hours on reasonable notice to recover any such Property.

B8.2 The Supplier does not have a lien or any other interest on the Property and the Supplier at all times possesses the Property as fiduciary agent and bailee of the Authority. The Supplier shall take all reasonable steps to ensure that the title of the Authority to the Property and the exclusion of any such lien or other interest are brought to the notice of all Sub-Contractors and other appropriate persons and shall, at the Authority's request, store the Property separately and ensure that it is clearly identifiable as belonging to the Authority.

B8.3 The Property is deemed to be in good condition when received by or on behalf of the Supplier unless the Supplier notifies the Authority otherwise within 5 Working Days of receipt.

B8.4 The Supplier shall maintain the Property in good order and condition (excluding fair wear and tear) and shall use the Property solely in connection with the Contract and for no other purpose without Approval.

B8.5 The Supplier shall ensure the security of all the Property whilst in its possession, either on the Premises or elsewhere during the supply of the Services, in accordance with the Authority's reasonable security requirements as required from time to time.

B8.6 The Supplier is liable for all loss of or damage to the Property, unless such loss or damage was caused by the Authority's negligence. The Supplier shall inform the Authority immediately of becoming aware of any defects appearing in, or losses or damage occurring to, the Property.

B9 Offers of Employment

B9.1 Neither Party shall, directly or indirectly, solicit or procure (otherwise than by general advertising or under TUPE, any employees or contractors (including the Staff) of the other Party who are directly employed or engaged in connection with the provision of the Services while such persons are employed or engaged and for a period of 6 Months thereafter.

B9.2 If either Party breaches the clause B9.1, it shall pay the other Party a sum equivalent to 20% of the annual base salary payable by the Party in breach in respect of the first year of person's employment.

B9.3 The Parties hereby agree that the sum specified in clause B9.2 is a reasonable pre-estimate of the loss and damage which the Party not in breach would suffer if there was a breach of clause B9.1.

B10 Employment

B10.1 No later than 12 Months prior to the end of the Term, the Supplier shall fully and accurately disclose to the Authority all information the Authority may reasonably request in relation to the Staff including the following:

(a) the total number of Staff whose employment/engagement terminates at the end of the Term, save for any operation of Law;

(b) the age, gender, salary or other remuneration, future pay settlements and redundancy and pensions entitlement of the Staff referred to in clause B10.1 (a);

(c) the terms and conditions of employment/engagement of the Staff referred to in clause B10.1 (a), their job titles and qualifications;

(d) their immigration status;

(e) details of any current disciplinary or grievance proceedings ongoing or circumstances likely to give rise to such proceedings and details of any claims current or threatened; and

(f) details of all collective agreements with a brief summary of the current state of negotiations with any such bodies and with details of any current industrial disputes and claims for recognition by any trade union.

B10.2 At intervals determined by the Authority (which shall not be more frequent than once every 30 days) the Supplier shall give the Authority updated TUPE Information.

B10.3 Each time the Supplier supplies TUPE Information to the Authority it warrants its completeness and accuracy and the Authority may assign the benefit of this warranty to any Replacement Supplier.

B10.4 The Authority may use TUPE Information it receives from the Supplier for the purposes of TUPE and/or any retendering process in order to ensure an effective handover of all work in progress at the end of the Term. The Supplier shall provide the Replacement Supplier with such assistance as it shall reasonably request.

B10.5 If TUPE applies to the transfer of the Services on termination of the Contract, the Supplier indemnifies and keeps indemnified the Authority, the Crown and any Replacement Supplier against all actions, suits, claims, demands, losses, charges, damages, costs and expenses and other liabilities which the Authority or the Crown or any Replacement Supplier may suffer or incur as a result of or in connection with:

(a) the provision of TUPE Information;

(b) any claim or demand by any Employee (whether in contract, tort or under statute) in each case arising directly or indirectly from any act, fault or omission of the Supplier or any Sub-Contractor in respect of any Employee on or before the end of the Term;

(c) any failure by the Supplier or any Sub-Contractor to comply with its obligations under regulations 13 or 14 of TUPE or any award of compensation under regulation 15 of TUPE save where such failure arises from the failure of the Authority or a Replacement Supplier to comply with its duties under regulation 13 of TUPE;

(d) any claim (including any individual employee entitlement under or consequent on such a claim) by any trade union or other body or person representing any Employees arising from or connected with any failure by the Supplier or any Sub-Contractor to comply with any legal obligation to such trade union, body or person; and

(e) any claim by any person who is transferred by the Supplier to the Authority and/or a Replacement Supplier whose name is not included in the list of Employees.

B10.6 If the Supplier is aware that TUPE Information has become inaccurate or misleading, it shall notify the Authority and provide the Authority with up to date and accurate TUPE Information.

B10.7 This clause B10 applies during the Term and indefinitely thereafter.

B10.8 The Supplier undertakes to the Authority that, during the 12 Months prior to the end of the Term the Supplier shall not (and shall procure that any Sub-Contractor shall not) without Approval (such Approval not to be unreasonably withheld or delayed):

(a) amend or vary (or purport to amend or vary) the terms and conditions of employment or engagement (including, for the avoidance of doubt, pay) of any Staff (other than where such amendment or variation has previously been agreed between the Supplier and the Staff in the normal course of business and where any such amendment or variation is not in any way related to the transfer of the Services);

(b) terminate or give notice to terminate the employment or engagement of any Staff (other than in circumstances in which the termination is for reasons of misconduct or lack of capability);

(c) transfer away, remove, reduce or vary the involvement of any other Staff from or in the provision of the Services (other than where such transfer or removal: (i) was planned as part of the individual's career development; (ii) takes place in the normal course of business; and (iii) will not have any adverse impact upon the delivery of the Services by the Supplier, (provided that any such transfer, removal, reduction or variation is not in any way related to the transfer of the Services); or

(d) recruit or bring in any new or additional individuals to provide the Services who were not already involved in providing the Services prior to the relevant period.

B11 Implementation

B11.1 The Parties shall comply with the provisions of Schedule 10 (Implementation Plan) in relation to the agreement and maintenance of the Implementation Plan.

B11.2 The Supplier shall:

(a) comply with the Implementation Plan; and

(b) ensure that each Milestone is achieved on or before its Milestone Date.

B11.3 If the Supplier becomes aware that there is, or there is reasonably likely to be, a Delay:

(a) it shall:

(i) notify the Authority in accordance with Clause F1.1 (Contract Performance); and

(ii) comply with Clause F1 (Contract Performance) in order to address the impact of the Delay or anticipated Delay; and

(iii) use all reasonable endeavours to eliminate or mitigate the consequences of any Delay or anticipated Delay; and

(b) if the Delay or anticipated Delay relates to a Key Milestone, the provisions of Clause F2 (Remedies) shall apply.

C PAYMENT

C1 Payment and VAT

C1.1 The Supplier shall submit invoices to the Authority in accordance with this clause C1 and Schedule 2.

C1.2 The Authority issues Purchase Orders using Basware and, unless Approved otherwise, the Supplier shall, when invited, register on Basware.

C1.3 If the Supplier registers on Basware, a Valid Invoice is an invoice issued through Basware, unless the invoice contains:

(a) additional lines not included in the relevant Purchase Order;

(b) line descriptions which have been materially altered so that they no longer match the equivalent description in the relevant Purchase Order; or

(c) Prices and/or volumes which have been increased without Approval.

C1.4 If, with Approval, the Supplier does not register on Basware, a Valid Invoice is an invoice which complies with clauses 1.5 to 1.7.

C1.5 Other than invoices submitted through Basware, all invoices submitted to the Authority must clearly state the word 'invoice' and contain:

(a) a unique identification number (invoice number);

(b) the Supplier's name, address and contact information;

(c) the name and address of the department/agency in the Authority with which the Supplier is working;

(d) a clear description of the services being invoiced for;

(e) the date the services were provided;

(f) the date of the invoice;

(g) the amount being charged;

(h) VAT amount if applicable;

(i) the total amount owed;

(j) the Purchase Order number; and

(k) the amount of the invoice in sterling or any other currency which is Approved.

C1.6 Other than invoices submitted through Basware, all invoices submitted to the Authority must meet the following criteria:

(a) email size must not exceed 4mb;

(b) one invoice per file attachment (PDF). Multiple invoices can be attached as separate files;

(c) any supporting information, backing data etc. must be contained within the invoice PDF file;

(d) not contain any lines for items which are not on the Purchase Order;

(e) replicate, as far as possible, the structure of and the information contained in the Purchase Order in respect of the number of lines, line descriptions, price and quantity; and

(f) if required by the Authority, be submitted in a structured electronic invoice in an Electronic Data Interchange or XML formats.

C1.7 Other than invoices submitted through Basware, all invoices submitted to the Authority must, if requested by the Authority, include:

(a) timesheets for Staff engaged in providing the Services signed and dated by the Authority's representative on the Premises on the day;

(b) the name of the individuals to whom the timesheet relates and hourly rates for each;

(c) identification of which individuals are Supplier's staff and which are Sub-Contractors' staff;

(d) the address of the Premises and the date on which work was undertaken;

(e) the time spent working on the Premises by the individuals concerned;

(f) details of the type of work undertaken by the individuals concerned;

(g) details of plant or materials operated and on standby;

(h) separate identification of time spent travelling and/or meal or rest breaks; and

(i) if appropriate, details of journeys made and distances travelled.

C1.8 The Authority shall not pay an invoice which is not a Valid Invoice.

C1.9 The Authority shall not pay the Supplier's overhead costs unless Approved and overhead costs include, without limitation: facilities, utilities, insurance, tax, head office overheads, indirect staff costs and other costs not specifically and directly ascribable solely to the provision of the Services.

C1.10 If Schedule 2 expressly provides that the Authority may be charged for plant which is on standby then if plant was waiting to be transferred between Premises or if the Authority has instructed that the plant is retained on the Premises then a standby charge of 60% of agreed rates may be made in respect of such relevant periods if supported by timesheets.

C1.11 The Authority shall not pay a stand-by rate if plant is on standby because no work was being carried out on the Premises at that time or no operator or other relevant staff were available (unless the standby is because the Supplier is awaiting licensing of the Premises on the Authority's instructions).

C1.12 The Authority shall not pay for plant or equipment which is stood down during any notice period pursuant to clauses H1, H2 and/or H3 and the Supplier shall mitigate such costs as far as is reasonably possible, for example, by reutilising Staff, plant, materials and services on other contracts.

C1.13 For the avoidance of doubt, the Core Requirement Pricing is inclusive of any and all expenses that the Supplier may incur as part of providing the Core Services No expenses can be claimed by the Supplier for the Core Services.

C1.13A In respect of Ad Hoc Projects, the Supplier may claim reasonable expenses only if they are clearly identified, supported by original receipts and Approved as part of the

Supplier's response to the Authority's RFQ for Ad Hoc Projects. An invoice for Ad Hoc Projects which does not comply with this clause C1.13A is not a Valid Invoice.

C1.14 If the Authority pays the Supplier prior to the submission of a Valid Invoice this payment is on account of and deductible from the next payment to be made.

C1.15 If any overpayment has been made or the payment or any part is not supported by a Valid Invoice the Authority may recover this payment against future invoices raised or directly from the Supplier. All payments made by the Authority to the Supplier are on an interim basis pending final resolution of an account with the Supplier in accordance with the terms of this clause C1.

C1.16 The Supplier shall:

(a) add VAT to the Price at the prevailing rate as applicable and show the amount of VAT payable separately on all invoices as an extra charge. If the Supplier fails to show VAT on an invoice, the Authority is not, at any later date, liable to pay the Supplier any additional VAT;

(b) ensure that a provision is included in all Sub-Contracts which requires payment to be made of all sums due to Sub-Contractors within 30 days from the receipt of a valid invoice; and

(c) not suspend the Services unless the Supplier is entitled to terminate the Contract under clause H2.3 for failure to pay undisputed sums of money.

C1.17 The Supplier indemnifies the Authority on a continuing basis against any liability, including any interest, penalties or costs incurred, which 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 the Contract. Any amounts due under this clause shall be paid by the Supplier to the Authority not less than 5 Working Days before the date upon which the tax or other liability is payable by the Authority.

C1.18 The Authority shall:

(a) in addition to the Price and following receipt of a Valid Invoice, pay the Supplier a sum equal to the VAT chargeable on the value of the Services supplied in accordance with the Contract; and

(b) pay all sums due to the Supplier within 30 days of receipt of a Valid Invoice unless an alternative arrangement has been Approved.

C1.19 If the Authority fails to pay any undisputed invoices under the Contract, the Supplier may 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.

C2 Recovery of Sums Due

C2.1 If under the Contract any sum of money is recoverable from or payable by the Supplier to the Authority (including any sum which the Supplier is liable to pay to the Authority in respect of any breach of the Contract), the Authority may unilaterally deduct that

sum from any sum then due, or which at any later time may become due to the Supplier from the Authority under the Contract or under any other agreement with the Authority or the Crown.

C2.2 Any overpayment by either Party, whether of the Price or of VAT or otherwise, is a sum of money recoverable by the Party who made the overpayment from the Party in receipt of the overpayment.

C2.3 The Supplier shall make all payments due to the Authority without any deduction whether by way of set-off, counterclaim, discount, abatement or otherwise unless the Supplier has a valid court order requiring an amount equal to such deduction to be paid by the Authority to the Supplier.

C2.4 All payments due shall be made within a reasonable time unless otherwise specified in the Contract, in cleared funds, to such bank or building society account as the recipient Party may from time to time direct.

C3 Price During Extension

Subject to Schedule 2 and clause F4 (Change), the Price applies for the Initial Term and until the end of any Extension or such earlier date of termination or partial termination of the Contract in accordance with the Law or the Contract.

D PROTECTION OF INFORMATION

D1 Authority Data

D1.1 The Supplier shall:

(a) not store, copy, disclose, or use the Authority Data except as necessary for the performance by the Supplier of its obligations under the Contract or as otherwise Approved;

(b) preserve the integrity of Authority Data and prevent the corruption or loss of Authority Data;

(c) not delete or remove any proprietary notices contained within or relating to the Authority Data;

(d) to the extent that Authority Data is held and/or processed by the Supplier, supply Authority Data to the Authority as requested by the Authority in the format specified in the Specification;

(e) perform secure back-ups of all Authority Data and ensure that up-to-date back-ups are stored securely off-site. The Supplier shall ensure that such back-ups are made available to the Authority immediately upon request;

(f) 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 Policy Framework;

(g) identify, and disclose to the Authority on request those members of Staff with access to or who are involved in handling Authority Data;

(h) on request, give the Authority details of its policy for reporting, managing and recovering from information risk incidents, including losses of Personal Data, and its procedures for reducing risk;

(i) notify the Authority immediately and inform the Authority of the remedial action the Supplier proposes to take if it has reason to believe that Authority Data has or may become corrupted, lost or sufficiently degraded in any way for any reason; and

(j) comply with Schedule 6 (Security Requirements and Policy).

D1.2 If Authority Data is corrupted, lost or sufficiently degraded as a result of the Supplier's Default so as to be unusable, the Authority may:

(a) require the Supplier (at the Supplier's cost) to restore or procure the restoration of Authority Data and the Supplier shall do so promptly; and/or

(b) itself restore or procure the restoration of Authority Data and be repaid by the Supplier any reasonable costs incurred in doing so.

D2 Data Protection and Privacy

D2.1 The Parties acknowledge that for the purposes of Data Protection Law, the Authority is the Controller and the Supplier is the Processor. The only processing which the Authority has authorised the Supplier to do is listed in Schedule 9 and may not be determined by the Supplier.

D2.2 The Supplier shall:

(a) notify the Authority immediately if it considers any Authority instructions infringe Data Protection Law;

(b) at its own cost, provide all reasonable assistance to the Authority in the preparation of any DPIA prior to starting any processing. Such assistance may, at the Authority's discretion, include:

i) a systematic description of the envisaged Processing and the purpose of the Processing;

ii) an assessment of the necessity and proportionality of the Processing operations in relation to the Services;

iii) an assessment of the risks to the rights and freedoms of Data Subjects; and

iv) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data

(c) in relation to any Personal Data Processed in connection with its obligations under the Contract:

i) Process that Personal Data only in accordance with Schedule 9 unless the Supplier is required to do otherwise by Law. If it is so required, the Supplier shall promptly notify the Authority before processing the Personal Data unless prohibited by Law; and

ii) ensure that it has in place Protective Measures which are appropriate to protect against a Data Loss Event which the Authority may reasonably reject. If the Authority reasonably rejects the Protective Measures put in place by the Supplier, the Supplier shall propose alternative Protective Measures to the satisfaction of the Authority. If the Authority does not reject the proposed Protective Measures this does not mean they are Approved. Protective Measures must take account of the nature of the Personal Data to be protected, the harm that might result from a Data Loss Event, the state of technological development and the cost of implementing any measures

(d) ensure that:

i) Staff do not Process Personal Data except in accordance with the Contract (and in particular Schedule 9;

ii) it takes all reasonable steps to ensure the reliability and integrity of any Staff who have access to Personal Data and ensure that they:

A) are aware of and comply with the Supplier's duties under this clause D2;

B) are subject to appropriate confidentiality undertakings with the Supplier or any Sub-processor;

C) are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third party unless directed in writing to do so by the Authority or as otherwise allowed under the Contract;

D) have undergone adequate training in the use, care, protection and handling of the Personal Data

(e) where the Personal Data is subject to UK GDPR, not transfer the Personal Data outside of the UK unless Approved and:

i) the destination country has been recognised as adequate by the Government in accordance with Article 45 of the UK GDPR (or s.74 of DPA);

ii) the Authority or the Supplier has provided appropriate safeguards in relation to the transfer (whether in accordance with Article 46 of the UK GDPR or s.75 of the DPA) as determined by the Authority;

iii) the Data Subject has enforceable rights and effective legal remedies;

iv) the Supplier complies with its obligations under Data Protection Law by providing an appropriate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the Authority in meeting its obligations); and

v) the Supplier complies with any reasonable instructions notified to it in advance by the Authority with respect to the processing of the Personal Data

(f) at the written direction of the Authority, delete or return Personal Data (and any copies of it) to the Authority on termination of the Contract unless the Supplier is required by Law to retain the Personal Data;

(g) subject to clause D2.3, notify the Authority immediately if it:

i) receives a Data Subject Request (or purported Data Subject Request);

ii) receives a request to rectify, block or erase any Personal Data;

iii) receives any other request, complaint or communication relating to either Party's obligations under Data Protection Law;

iv) receives any communication from the ICO or any other regulatory authority in connection with Personal Data Processed under the Contract;

v) receives a request from any third party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law; or

vi) becomes aware of a Data Loss Event.

D2.3 The Supplier's obligation to notify under clause D2.2 (g) includes the provision of further information to the Authority as details become available.

D2.4 Taking into account the nature of the Processing, the Supplier shall provide the Authority with full assistance in relation to either Party's obligations under Data Protection Law and any complaint, communication or request made under clause D2.2 (g) (and insofar as possible within the timescales reasonably required by the Authority) including by promptly providing:

(a) the Authority with full details and copies of the complaint, communication or request;

(b) such assistance as is reasonably requested by the Authority to enable the Authority to comply with a Data Subject Request within the relevant timescales set out in Data Protection Law;

(c) the Authority, at its request, with any Personal Data it holds in relation to a Data Subject;

(d) assistance as requested by the Authority following any Data Loss Event; and

(e) assistance as requested by the Authority with respect to any request from the ICO or any consultation by the Authority with the ICO.

D2.5 The Supplier shall maintain complete and accurate records and information to demonstrate its compliance with clause D2. This requirement does not apply if the Supplier employs fewer than 250 people unless the Authority determines that the processing:

(a) is not occasional;

(b) includes special categories of data as referred to in Article 9(1) of the UK GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the UK GDPR; or

(c) is likely to result in a risk to the rights and freedoms of Data Subjects.

D2.6 The Supplier shall allow audits of its Processing activity by the Authority or the Authority's designated auditor.

D2.7 The Supplier shall designate a Data Protection Officer if required by Data Protection Law.

D2.8 Before allowing any Sub-processor to Process any Personal Data in connection with the Contract, the Supplier shall:

(a) notify the Authority in writing of the intended Sub-processor and Processing:

(b) obtain Approval;

(c) enter into a written agreement with the Sub-processor which gives effect to the terms set out in clause D2 such that they apply to the Sub-processor; and

(d) provide the Authority with such information regarding the Sub-processor as the Authority reasonably requires.

D2.9 The Supplier remains fully liable for the acts and omissions of any Sub-processor.

D2.10 The Parties shall take account of any guidance published by the ICO and, notwithstanding the provisions of clause F4, the Authority may on not less than 30 Working Days' notice to the Supplier amend the Contract to ensure that it complies with any guidance published by the ICO.

D2.11 In relation to Processing for Law Enforcement Purposes, the Supplier shall:

(a) maintain logs for its automated Processing operations in respect of:

i) collection;

ii) alteration;

iii) consultation;

iv) disclosure (including transfers);

v) combination; and

vi) erasure.

(together the "**Logs**").

(b) ensure that:

i) the Logs of consultation make it possible to establish the justification for, and date and time of, the consultation; and as far as possible, the identity of the person who consulted the data;

ii) the Logs of disclosure make it possible to establish the justification for, and date and time of, the disclosure; and the identity of the recipients of the data; and

iii) the Logs are made available to the ICO on request

(c) use the Logs only to:

i) verify the lawfulness of Processing;

ii) assist with self-monitoring by the Authority or (as the case may be) the Supplier, including the conduct of internal disciplinary proceedings;

iii) ensure the integrity of Personal Data; and

iv) assist with criminal proceedings

(d) as far as possible, distinguish between Personal Data based on fact and Personal Data based on personal assessments; and

(e) where relevant and as far as possible, maintain a clear distinction between Personal Data relating to different categories of Data Subject, for example:

i) persons suspected of having committed or being about to commit a criminal offence;

ii) persons convicted of a criminal offence;

iii) persons who are or maybe victims of a criminal offence; and

iv) witnesses or other persons with information about offences.

D2.12 This clause D2 applies during the Term and indefinitely after its expiry.

D3 Official Secrets Acts and Finance Act

D3.1 The Supplier shall comply with:

(a) the Official Secrets Acts 1911 to 1989; and

(b) section 182 of the Finance Act 1989.

D4 Confidential Information

D4.1 Except to the extent set out in clause D4 or if disclosure or publication is expressly allowed elsewhere in the Contract each Party shall treat all Confidential Information belonging to the other Party as confidential and shall not disclose any Confidential Information belonging to the other Party to any other person without the other Party's consent, except to such persons and to such extent as may be necessary for the performance of the Party's obligations under the Contract.

D4.2 The Supplier hereby gives its consent for the Authority to publish the whole Contract (but with any information which is Confidential Information belonging to the Authority redacted) including from time to time agreed changes to the Contract, to the general public.

D4.3 If required by the Authority, the Supplier shall ensure that Staff, professional advisors and consultants sign a non-disclosure agreement prior to commencing any work in connection with the Contract in a form approved by the Authority. The Supplier shall maintain a list of the non-disclosure agreements completed in accordance with this clause.

D4.4 If requested by the Authority, the Supplier shall give the Authority a copy of the list and, subsequently upon request by the Authority, copies of such of the listed non-disclosure agreements as required by the Authority. The Supplier shall ensure that Staff, professional advisors and consultants are aware of the Supplier's confidentiality obligations under the Contract.

D4.5 The Supplier may disclose the Authority's Confidential Information only to Staff who are directly involved in providing the Services and who need to know the information, and shall ensure that such Staff are aware of and shall comply with these obligations as to confidentiality.

D4.6 The Supplier shall not, and shall procure that the Staff do not, use any of the Authority's Confidential Information received otherwise than for the purposes of the Contract.

D4.7 Clause D4.1 shall not apply to the extent that:

(a) such disclosure is a requirement of Law placed upon the Party making the disclosure, including any requirements for disclosure under the FOIA or the EIR;

(b) such information was in the possession of the Party making the disclosure without obligation of confidentiality prior to its disclosure by the information owner;

(c) such information was obtained from a third party without obligation of confidentiality;

(d) such information was already in the public domain at the time of disclosure otherwise than by a breach of the Contract; or

(e) it is independently developed without access to the other Party's Confidential Information.

D4.8 Nothing in clause D4.1 prevents the Authority disclosing any Confidential Information obtained from the Supplier:

(a) for the purpose of the examination and certification of the Authority's accounts;

(b) for the purpose of any examination pursuant to section 6(1) of the National Audit Act 1983 of the economy, efficiency and effectiveness with which the Authority has used its resources;

(c) to Parliament and Parliamentary committees;

(d) to any Crown Body or any Contracting Authority and the Supplier hereby acknowledges that all Government departments or Contracting Authorities receiving such Confidential Information may further disclose the Confidential Information to other Government departments or other Contracting Authorities on the basis that the information is confidential and is not to be disclosed to a third party which is not part of any Government department or any Contracting Authority; or

(e) to any consultant, contractor or other person engaged by the Authority

provided that in disclosing information under clauses D4.8 (d) and (e) the Authority discloses only the information which is necessary for the purpose concerned and requests that the information is treated in confidence and that a confidentiality undertaking is given where appropriate.

D4.9 Nothing in clauses D4.1 to D4.6 prevents either Party from using any techniques, ideas or Know-How gained during the performance of its obligations under the Contract in the course of its normal business, to the extent that this does not result in a disclosure of the other Party's Confidential Information or an infringement of the other Party's Intellectual Property Rights.

D4.10 The Authority shall use reasonable endeavours to ensure that any Government department, Contracting Authority, employee, third party or Sub-Contractor to whom the Supplier's Confidential Information is disclosed pursuant to clause D4.8 is made aware of the Authority's obligations of confidentiality.

D4.11 If the Supplier does not comply with clauses D4.1 to D4.8 the Authority may terminate the Contract immediately on notice.

D4.12 To ensure that no unauthorised person gains access to any Confidential Information or any data obtained in the supply of the Services, the Supplier shall maintain adequate security arrangements that meet the requirements of professional standards and best practice.

D4.13 The Supplier shall:

(a) immediately notify the Authority of any breach of security in relation to Confidential Information and all data obtained in the supply of the Services and will keep a record of such breaches;

(b) use best endeavours to recover such Confidential Information or data however it may be recorded;

(c) co-operate with the Authority in any investigation as a result of any breach of security in relation to Confidential Information or data; and

(d) at its own expense, alter any security systems at any time during the Term at the Authority's request if the Authority reasonably believes the Supplier has failed to comply with clause D4.12.

D5 Freedom of Information

D5.1 The Supplier acknowledges that the Authority is subject to the requirements of the FOIA and the EIR.

D5.2 The Supplier shall transfer to the Authority all Requests for Information that it receives as soon as practicable and in any event within 2 Working Days of receipt and shall:

(a) give the Authority a copy of all Information in its possession or control in the form that the Authority requires within 5 Working Days (or such other period as the Authority may specify) of the Authority's request;

(b) provide all necessary assistance as reasonably requested by the Authority to enable the Authority to comply with its obligations under the FOIA and EIR; and

(c) not respond directly to a Request for Information unless authorised to do so in writing by the Authority.

D5.3 The Authority shall determine in its absolute discretion and notwithstanding any other provision in the Contract or any other agreement whether the Commercially Sensitive Information and any other Information is exempt from disclosure in accordance with the FOIA and/or the EIR.

D6 Publicity, Media and Official Enquiries

D6.1 The Supplier shall not:

(a) make any press announcements or publicise the Contract or its contents in any way;

(b) use the Authority's name, brand or logo in any publicity, promotion, marketing or announcement of order; or

(c) use the name, brand or logo of any of the Authority's agencies or arms-length bodies in any publicity, promotion, marketing or announcement of orders

without Approval.

D6.2 Each Party acknowledges that nothing in the Contract either expressly or impliedly constitutes an endorsement of any products or services of the other Party (including

the Services and the ICT Environment) and each Party shall not conduct itself in such a way as to imply or express any such approval or endorsement.

D6.3 The Supplier shall use reasonable endeavours to ensure that its Staff and professional advisors comply with clause D6.1.

E INTELLECTUAL PROPERTY

E1 Intellectual Property Rights

E1.1 All Intellectual Property Rights in:

(a) the Results; or

(b) any guidance, specifications, reports, studies, instructions, toolkits, plans, data, drawings, databases, patents, patterns, models, designs or other material which is furnished to or made available to the Supplier by or on behalf of the Authority (together with the Results, the "**IP Materials**")

shall vest in the Authority (save for Copyright and Database Rights which shall vest in Her Majesty the Queen) and the Supplier shall not, and shall ensure that the Staff shall not, use or disclose any IP Materials without Approval save to the extent necessary for performance by the Supplier of its obligations under the Contract.

E1.2 The Supplier hereby assigns:

(a) to the Authority, with full title guarantee, all Intellectual Property Rights (save for Copyright and Database Rights) which may subsist in the IP Materials. This assignment shall take effect on the date of the Contract or (in the case of rights arising after the date of the Contract) as a present assignment of future rights that will take effect immediately on the coming into existence of the Intellectual Property Rights produced by the Supplier; and

(b) to Her Majesty the Queen, with full title guarantee, all Copyright and Database Rights which may subsist in the IP Materials

and shall execute all documents and do all acts as are necessary to execute these assignments.

E1.3 The Supplier shall:

(a) waive or procure a waiver of any moral rights held by it or any third party in copyright material arising as a result of the Contract or the performance of its obligations under the Contract;

(b) ensure that the third-party owner of any Intellectual Property Rights that are or which may be used to perform the Services grants to the Authority a non-exclusive licence or, if itself a licensee of those rights, shall grant to the Authority an authorised sub-licence, to use, reproduce, modify, develop and maintain the Intellectual Property Rights in the same. Such licence or sub-licence shall be

non-exclusive, perpetual, royalty-free, worldwide and irrevocable and include the right for the Authority to sub-license, transfer, novate or assign to other Contracting Authorities, the Crown, the Replacement Supplier or to any other third-party supplying goods and/or services to the Authority ("**Indemnified Persons**");

(c) not infringe any Intellectual Property Rights of any third party in supplying the Services; and

(d) during and after the Term, indemnify and keep indemnified the Authority and Indemnified Persons from and against all actions, suits, claims, demands, losses, charges, damages, costs and expenses and other liabilities which the Authority and Indemnified Persons may suffer or incur as a result of or in connection with any breach of clause E1.3, except to the extent that any such claim results directly from:

i) items or materials based upon designs supplied by the Authority; or

ii) the use of data supplied by the Authority which is not required to be verified by the Supplier under any provision of the Contract.

E1.4 The Authority shall notify the Supplier in writing of any claim or demand brought against the Authority or Indemnified Person for infringement or alleged infringement of any Intellectual Property Right in materials supplied and/or licensed by the Supplier to the Authority.

E1.5 The Supplier shall at its own expense conduct all negotiations and any litigation arising in connection with any claim, demand or action by any third party for infringement or alleged infringement of any third party Intellectual Property Rights (whether by the Authority, the Supplier or Indemnified Person) arising from the performance of the Supplier's obligations under the Contract (**"Third Party IP Claim**"), provided that the Supplier shall at all times:

(a) consult the Authority on all material issues which arise during the conduct of such litigation and negotiations;

(b) take due and proper account of the interests of the Authority; and

(c) not settle or compromise any claim without Approval (not to be unreasonably withheld or delayed).

E1.6 The Authority shall, at the request of the Supplier, afford to the Supplier all reasonable assistance for the purpose of contesting any Third-Party IP Claim and the Supplier shall indemnify the Authority for all costs and expenses (including, but not limited to, legal costs and disbursements) incurred in doing so. The Supplier is not required to indemnify the Authority under this clause in relation to any costs and expenses to the extent that such arise directly from the matters referred to in clauses E1.3 (d) i) and ii).

E1.7 The Authority shall not, without the Supplier's consent, make any admissions which may be prejudicial to the defence or settlement of any Third-Party IP Claim.

E1.8 If any Third-Party IP Claim is made or in the reasonable opinion of the Supplier is likely to be made, the Supplier shall notify the Authority and any relevant Indemnified

Person, at its own expense and subject to Approval (not to be unreasonably withheld or delayed), shall (without prejudice to the rights of the Authority under clauses E1.3 (b) and G2.1 (g)) use its best endeavours to:

(a) modify any or all of the Services without reducing the performance or functionality of the same, or substitute alternative services of equivalent performance and functionality, so as to avoid the infringement or the alleged infringement; or

(b) procure a licence to use the Intellectual Property Rights and supply the Services which are the subject of the alleged infringement, on terms which are acceptable to the Authority

and if the Supplier is unable to comply with clauses E1.8 (a) or (b) within 20 Working Days of receipt by the Authority of the Supplier's notification the Authority may terminate the Contract immediately by notice to the Supplier.

E1.9 The Supplier grants to the Authority and, if requested by the Authority, to a Replacement Supplier, a royalty-free, irrevocable, worldwide, non-exclusive licence (with a right to sub-license) to use any Intellectual Property Rights that the Supplier owned or developed prior to the Commencement Date and which the Authority (or the Replacement Supplier) reasonably requires in order for the Authority to exercise its rights under, and receive the benefit of, the Contract (including, without limitation, the Services).

F CONTROL OF THE CONTRACT

F1 Contract Performance

F1.1 The Supplier shall immediately inform the Authority if any of the Services are not being or are unable to be performed, the reasons for non-performance, any corrective action and the date by which that action will be completed.

F1.2 At or around 6 Months from the Commencement Date and each anniversary of the Commencement Date thereafter, the Authority may carry out a review of the performance of the Supplier (a **"Review"**). Without prejudice to the generality of the foregoing, the Authority may in respect of the period under review consider such items as (but not limited to):

a) the Supplier's delivery of the Services;

b) the Supplier's contribution to innovation in the Authority; whether the Services provide the Authority with best value for money; consideration of any changes which may need to be made to the Services;

c) a review of future requirements in relation to the Services; and

d) progress against Milestones and Key Milestones.

F1.3 The Supplier shall provide at its own cost any assistance reasonably required by the Authority to perform Reviews including the provision of data and information.

F1.4 The Authority may produce a report (a "**Review Report**") of the results of each Review stating any areas of exceptional performance and areas for improvement in the provision of the Services and where there is any shortfall in any aspect of performance reviewed as against the Authority's expectations and the Supplier's obligations under the Contract.

F1.5 The Authority shall give the Supplier a copy of the Review Report (if applicable). The Authority shall consider any Supplier comments and may produce a revised Review Report.

F1.6 The Supplier shall, within 10 Working Days of receipt of the Review Report (revised as appropriate) provide the Authority with a plan to address resolution of any shortcomings and implementation of improvements identified by the Review Report.

F1.7 Actions required to resolve shortcomings and implement improvements (either as a consequence of the Supplier's failure to meet its obligations under the Contract identified by the Review Report, or those which result from the Supplier's failure to meet the Authority's expectations notified to the Supplier or of which the Supplier ought reasonably to have been aware) shall be implemented at no extra cost to the Authority.

F1.8 At any point at the request of the Authority to discuss the performance of the Contract, the Supplier shall attend progress meetings (" **Progress Meetings**") with the Authority at the frequency and times specified by the Authority and shall ensure that its representatives are suitably qualified to attend such meetings.

F1.9 The Supplier shall submit a report (a "**Progress Report**") of the performance of the Contract to the Authority at the times and in the format specified by the Authority.

F2 Remedies

F2.1 If the Authority reasonably believes the Supplier has committed a Material Breach it may, without prejudice to its rights under clause H2 (Termination on Default), do any of the following:

(a) without terminating the Contract, itself supply or procure the supply of all or part of the Services until such time as the Supplier has demonstrated to the Authority's reasonable satisfaction that the Supplier will be able to supply the Services in accordance with the Specification;

(b) without terminating the whole of the Contract, terminate the Contract in respect of part of the Services only (whereupon a corresponding reduction in the Price shall be made) and thereafter itself supply or procure a third party to supply such part of the Services;

(c) withhold or reduce payments to the Supplier in such amount as the Authority reasonably deems appropriate in each particular case; and/or

(d) terminate the Contract in accordance with clause H2.

F2.2 Without prejudice to its right under clause C3 (Recovery of Sums Due), the Authority may charge the Supplier for any costs reasonably incurred and any reasonable administration costs in respect of the supply of any part of the Services by the Authority or a third party to the extent that such costs exceed the payment which would otherwise have been payable to the Supplier for such part of the Services.

F2.3 If the Authority reasonably believes the Supplier has failed to supply all or any part of the Services in accordance with the Contract, professional or Good Industry Practice which could reasonably be expected of a competent and suitably qualified person, or any legislative or regulatory requirement, the Authority may give the Supplier notice specifying the way in which its performance falls short of the requirements of the Contract or is otherwise unsatisfactory.

F2.4 If the Supplier has been notified of a failure in accordance with clause F2.3 the Authority may:

(a) direct the Supplier to identify and remedy the failure within such time as may be specified by the Authority and to apply all such additional resources as are necessary to remedy that failure at no additional charge to the Authority within the specified timescale; and/or

(b) withhold or reduce payments to the Supplier in such amount as the Authority deems appropriate in each particular case until such failure has been remedied to the satisfaction of the Authority.

F2.5 If the Supplier has been notified of a failure in accordance with clause F2.3, it shall:

(a) use all reasonable endeavours to immediately minimise the impact of such failure to the Authority and to prevent such failure from recurring; and

(b) immediately give the Authority such information as the Authority may request regarding what measures are being taken to comply with the obligations in clause F2.5 and the progress of those measures until resolved to the satisfaction of the Authority.

F2.6 If, having been notified of any failure, the Supplier does not remedy it in accordance with clause F2.5 in the time specified by the Authority, the Authority may treat the continuing failure as a Material Breach and may terminate the Contract immediately on notice to the Supplier.

F3 Transfer and Sub-Contracting

F3.1 Except where both clauses F3.9 and F3.10 apply, the Supplier shall not transfer, charge, assign, sub-contract or in any other way dispose of the Contract or any part of it without Approval. All such actions shall be evidenced in writing and shown to the Authority on request. Sub-contracting any part of the Contract does not relieve the Supplier of any of its obligations or duties under the Contract.

F3.2 The Supplier is responsible for the acts and/or omissions of its Sub-Contractors as though they are its own. If it is appropriate, the Supplier shall provide each Sub-Contractor with a copy of the Contract and obtain written confirmation from them that they will provide the Services fully in accordance with the Contract.

F3.3 The Supplier shall ensure that Sub-Contractors retain all records relating to the Services for at least 6 years from the date of their creation and make them available to the Authority on request in accordance with clause F5 (Audit). If any Sub-Contractor does not allow the Authority access to the records the Authority has no obligation to pay any claim or invoice made by the Supplier on the basis of such documents or work carried out by the Sub-Contractor.

F3.4 If the Authority has consented to the award of a Sub-Contract, the Supplier shall ensure that:

(a) the Sub-Contract contains:

i) a right for the Supplier to terminate if the Sub-Contractor does not comply with its legal obligations in connection with Data Protection Law, environmental, social or labour law; and

ii) obligations no less onerous on the Sub-Contractor than those on the Supplier under the Contract in respect of data protection in clauses D1 and D2

(b) the Sub-Contractor includes a provision having the same effect as set out in this clause F3.4 (a) in any Sub-Contract which it awards; and

(c) copies of each Sub-Contract are sent to the Authority immediately after their execution.

F3.5 Unless Approved otherwise, if the total value of the Contract over the Term is, or is likely to be, in excess of £5,000,000, the Supplier shall, in respect of Sub-Contract opportunities arising during the Term from or in connection with the provision of the Services:

(a) advertise on Contracts Finder those that have a value in excess of £25,000;

(b) within 90 days of awarding a Sub-Contract, update the notice on Contracts Finder with details of the Sub-Contractor;

(c) monitor the number, type and value of the Sub-Contract opportunities placed on Contracts Finder and awarded during the Term;

(d) provide reports on the information in clause F3.5 (c) to the Authority in the format and frequency reasonably specified by the Authority;

(e) promote Contracts Finder to its suppliers and encourage them to register on Contracts Finder; and

(f) ensure that each advertisement placed pursuant to F3.5 (a) includes a full and detailed description of the Sub-Contract opportunity with each of the mandatory fields being completed on Contracts Finder.

F3.6 The Supplier shall, at its own cost, supply to the Authority by the end of April each year for the previous Financial Year:

(a) the total revenue received from the Authority pursuant to the Contract;

(b) the total value of all its Sub-Contracts;

(c) the total value of its Sub-Contracts with SMEs; and

(d) the total value of its Sub-Contracts with VCSEs.

F3.7 The Authority may from time to time change the format and the content of the information required pursuant to clause F3.6.

F3.8 If the Authority believes there are:

(a) compulsory grounds for excluding a Sub-Contractor pursuant to regulation 57 of the Regulations, the Supplier shall replace or not appoint the Sub-Contractor; or

(b) non-compulsory grounds for excluding a Sub-Contractor pursuant to regulation 57 of the Regulations, the Authority may require the Supplier to replace or not appoint the Sub-Contractor and the Supplier shall comply with such requirement.

F3.9 Notwithstanding clause F3.1, the Supplier may assign to a third party (the "**Assignee**") the right to receive payment of the Price or any part thereof due to the Supplier (including any interest which the Authority incurs under clause C1 (Payment and VAT)). Any assignment under clause F3.9 is subject to:

(a) reduction of any sums in respect of which the Authority exercises its right of recovery under clause C2 (Recovery of Sums Due);

(b) all related rights of the Authority under the Contract in relation to the recovery of sums due but unpaid; and

(c) the Authority receiving notification under both clauses F3.10 and F3.11.

F3.10 If the Supplier assigns the right to receive the Price under clause F3.9, the Supplier or the Assignee shall notify the Authority in writing of the assignment and the date upon which the assignment becomes effective.

F3.11 The Supplier shall ensure that the Assignee notifies the Authority of the Assignee's contact information and bank account details to which the Authority can make payment.

F3.12 Clause C1 continues to apply in all other respects after the assignment and shall not be amended without Approval.

F3.13 Subject to clause F3.14, the Authority may assign, novate or otherwise dispose of its rights and obligations under the Contract or any part thereof to:

(a) any Contracting Authority;

(b) any other body established or authorised by the Crown or under statute in order substantially to perform any of the functions that had previously been performed by the Authority; or

(c) any private sector body which substantially performs the functions of the Authority

provided that any such assignment, novation or other disposal shall not increase the burden of the Supplier's obligations under the Contract.

F3.14 Any change in the legal status of the Authority such that it ceases to be a Contracting Authority shall not, subject to clause F3.15, affect the validity of the Contract and the Contract shall bind and inure to the benefit of any successor body to the Authority.

F3.15 If the rights and obligations under the Contract are assigned, novated or otherwise disposed of pursuant to clause F3.13 to a body which is not a Contracting Authority or if there is a change in the legal status of the Authority such that it ceases to be a Contracting Authority (in the remainder of this clause both such bodies being referred to as the **"Transferee"**):

(a) the rights of termination of the Authority in clauses H1 and H2 are available to the Supplier in respect of the Transferee; and

(b) the Transferee shall only be able to assign, novate or otherwise dispose of its rights and obligations under the Contract or any part thereof with the prior consent in writing of the Supplier.

F3.16 The Authority may disclose to any Transferee any Confidential Information of the Supplier which relates to the performance of the Supplier's obligations under the Contract. In such circumstances the Authority shall authorise the Transferee to use such Confidential Information only for purposes relating to the performance of the Supplier's obligations under the Contract and for no other purpose and shall take all reasonable steps to ensure that the Transferee gives a confidentiality undertaking in relation to such Confidential Information.

F3.17 Each Party shall at its own cost and expense carry out, or use all reasonable endeavours to ensure the carrying out of, whatever further actions (including the execution of further documents) the other Party reasonably requires from time to time for the purpose of giving that other Party the full benefit of the Contract.

F4 Change

F4.1 After the Commencement Date, either Party may request a Change subject to the terms of this clause F4.

F4.2 Either Party may request a Change by notifying the other Party in writing of the Change by completing the Change Request Form set out in Schedule 3. The Party requesting the Change shall give the other Party sufficient information and time to assess the extent and effect of the requested Change. If the receiving Party accepts the Change it shall confirm it in writing to the other Party.

F4.3 If the Supplier is unable to accept a Change requested by the Authority or if the Parties are unable to agree a change to the Price, the Authority may:

(a) allow the Supplier to fulfil its obligations under the Contract without the Change; or

(b) terminate the Contract immediately except where the Supplier has already delivered all or part of the Services or where the Supplier can show evidence of substantial work being carried out to fulfil the requirements of the Specification; and in such case the Parties shall attempt to agree upon a resolution to the matter. If a resolution cannot be reached, the matter shall be dealt with under the Dispute Resolution Procedure detailed in clause I2 (Dispute Resolution).

F4.4 A Change takes effect only when it is recorded in a CCN validly executed by both Parties.

F4.5 The Supplier is deemed to warrant and represent that the CCN has been executed by a duly authorised representative of the Supplier in addition to the warranties and representations set out in clause G2.

F4.6 Clauses F4.4 and F4.5 may be varied in an emergency if it is not practicable to obtain the Authorised Representative's approval within the time necessary to make the Change in order to address the emergency. In an emergency, Changes may be approved by a different representative of the Authority. However, the Authorised Representative may review such a Change and require a CCN to be entered into on a retrospective basis which may itself vary the emergency Change.

F5 Audit

F5.1 The Supplier shall:

(a) keep and maintain for 6 years after the end of the Term, or as long a period as may be agreed between the Parties, full and accurate records of its compliance with, and discharge of its obligations under the Contract including the Services supplied under it, all expenditure reimbursed by the Authority, and all payments made by the Authority;

(b) on request afford the Authority or the Authority's representatives such access to those records and processes as may be requested by the Authority in connection with the Contract; and

(c) make available to the Authority, free of charge, whenever requested, copies of audit reports obtained by the Supplier in relation to the Services.

F5.2 The Authority, acting by itself or through its duly authorised representatives and/or the National Audit Office, may, during the Term and for a period of 18 Months thereafter,

assess compliance by the Supplier of the Supplier's obligations under the Contract, including to:

(a) verify the accuracy of the Price and any other amounts payable by the Authority under the Contract;

(b) verify the Open Book Data;

(c) verify the Supplier's compliance with the Contract and applicable Law;

(d) identify or investigate actual or suspected fraud, impropriety or accounting mistakes or any breach or threatened breach of security and in these circumstances the Authority has no obligation to inform the Supplier of the purpose or objective of its investigations;

(e) identify or investigate any circumstances which may impact upon the financial stability of the Supplier and/or any guarantor or their ability to perform the Services;

(f) obtain such information as is necessary to fulfil the Authority's obligations to supply information for parliamentary, ministerial, judicial or administrative purposes;

(g) 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;

(h) enable the National Audit Office to carry out an examination pursuant to Section 6(1) of the National Audit Act 1983 of the economy, efficiency and effectiveness with which the Authority has used its resources;

(i) verify the accuracy and completeness of any management information or reports delivered or required by the Contract;

(j) review the Supplier's compliance with the Authority's policies and standards; and/or

(k) review the integrity, confidentiality and security of the Authority Data

and the Supplier (and its agents) shall permit access free of charge during normal business hours on reasonable notice to all such documents (including computerised documents and data) and other information as the Authority (or those acting on its behalf) may reasonably require for the purposes of conducting such an audit.

F5.3 The Supplier (and its agents) shall permit the Comptroller and Auditor General (and his appointed representatives) access free of charge during normal business hours on reasonable notice to all such documents (including computerised documents and data) and other information as the Comptroller and Auditor General may reasonably require for the purposes of conducting a financial audit of the Authority and for carrying out examinations into the economy, efficiency and effectiveness with which the Authority has used its resources. The Supplier shall provide such explanations as are reasonably required for these purposes.

F5.4 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. The Authority shall endeavour to (but is not obliged to) provide at least 15 Working Days' notice of its intention to conduct an audit.

F5.5 The Parties bear their own respective costs and expenses incurred in respect of compliance with their obligations under clause F5, 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.

G LIABILITIES

G1 Liability, Indemnity and Insurance

G1.1 Neither Party limits its liability for:

(a) death or personal injury caused by its negligence;

(b) fraud or fraudulent misrepresentation;

(c) any breach of any obligations implied by section 12 of the Sale of Goods Act 1979 or section 2 of the Supply of Goods and Services Act 1982;

(d) any breach of clauses D1, D2 or D4 or Schedules 6 or 8; or

(e) any liability to the extent it cannot be limited or excluded by Law.

G1.2 Subject to clauses G1.3 and G1.5, the Supplier indemnifies the Authority fully against all claims, proceedings, demands, charges, actions, damages, costs, breach of statutory duty, expenses and any other liabilities which may arise out of the supply, or the late or purported supply, of the Services or the performance or non-performance by the Supplier of its obligations under the Contract or the presence of the Supplier or any Staff on the Premises, including in respect of any death or personal injury, loss of or damage to property, financial loss arising from any advice given or omitted to be given by the Supplier, or any other loss which is caused directly by any act or omission of the Supplier.

G1.3 Subject to clause G1.1 the Supplier's aggregate liability in respect of the Contract does not REDACTED Under FOIA Section 43, Commercial Interests or payable to the Supplier.

G1.4 Subject to clause G1.1 the Authority's aggregate liability in respect of the Contract does not exceed REDACTED Under FOIA Section 43, Commercial Interests of the Contract.

G1.5 The Supplier is not responsible for any injury, loss, damage, cost or expense if and to the extent that it is caused by the negligence or wilful misconduct of the Authority or by breach by the Authority of its obligations under the Contract.

G1.6 The Authority may recover from the Supplier the following losses incurred by the Authority to the extent they arise as a result of a Default by the Supplier:

(a) any additional operational and/or administrative costs and expenses incurred by the Authority, including costs relating to time spent by or on behalf of the Authority in dealing with the consequences of the Default;

(b) any wasted expenditure or charges;

(c) the additional costs of procuring a Replacement Supplier for the remainder of the Term and or replacement deliverables which shall include any incremental costs associated with the Replacement Supplier and/or replacement deliverables above those which would have been payable under the Contract;

(d) any compensation or interest paid to a third party by the Authority; and

(e) any fine or penalty incurred by the Authority pursuant to Law and any costs incurred by the Authority in defending any proceedings which result in such fine or penalty.

G1.7 Subject to clauses G1.1 and G1.6, neither Party is liable to the other for any:

(a) loss of profits, turnover, business opportunities or damage to goodwill; or

(b) indirect, special or consequential loss.

G1.8 Unless otherwise specified by the Authority, the Supplier shall, with effect from the Commencement Date for such period as necessary to enable the Supplier to comply with its obligations herein, take out and maintain with a reputable insurance company a policy or policies of insurance providing an adequate level of cover in respect of all risks which may be incurred by the Supplier, arising out of the Supplier's performance of its obligations under the Contract including:

(a) if required by the Authority, appropriate, professional indemnity insurance in the sum of not less than REDACTED Under FOIA Section 43, Commercial Interests) for any advice given by the Supplier to the Authority;

(b) cover for death or personal injury, loss of or damage to property or any other loss; and

(c) employer's liability insurance in respect of Staff.

Such insurance policies shall be maintained for the duration of the Term and for a minimum of 6 years following the end of the Term.

G1.9 The Supplier shall give the Authority, on request, copies of all insurance policies referred to in this clause or a broker's verification of insurance to demonstrate that the appropriate cover is in place, together with receipts or other evidence of payment of the latest premiums due under those policies.

G1.10 If the Supplier does not have and maintain the insurances required by the Contract, the Authority may make alternative arrangements to protect its interests and may recover the costs of such arrangements from the Supplier.

G1.11 The provisions of any insurance or the amount of cover shall not relieve the Supplier of any liabilities under the Contract.

G1.12 The Supplier shall not take any action or fail to take any reasonable action, or (to the extent that it is reasonably within its power) permit anything to occur in relation to the Supplier, which would entitle any insurer to refuse to pay any claim under any insurance policy in which the Supplier is an insured, a co-insured or additional insured person.

G2 Warranties and Representations

G2.1 The Supplier warrants and represents on the Commencement Date and for the Term that:

(a) it has full capacity and authority and all necessary consents to enter into and perform the Contract and that the Contract is executed by a duly authorised representative of the Supplier;

(b) in entering the Contract, it has not committed any fraud;

(c) as at the Commencement Date, all information contained in the Tender or other offer made by the Supplier to the Authority remains true, accurate and not misleading, save as may have been specifically disclosed in writing to the Authority prior to execution of the Contract and in addition, that it will advise the Authority of any fact, matter or circumstance of which it may become aware which would render such information to be false or misleading;

(d) no claim is being asserted and no litigation, arbitration or administrative proceeding is in progress or, to the best of its knowledge and belief, pending or threatened against it or any of its assets which will or might have an adverse effect on its ability to perform its obligations under the Contract;

(e) it is not subject to any contractual obligation, compliance with which is likely to have a material adverse effect on its ability to perform its obligations under the Contract;

(f) no proceedings or other steps have been taken and not discharged (or, 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;

(g) it owns, or has obtained or is able to obtain valid licences for, all Intellectual Property Rights that are necessary for the performance of its obligations under the Contract;

(h) any person engaged by the Supplier shall be engaged on terms which do not entitle them to any Intellectual Property Right in any IP Materials;

(i) in the 3 years (or period of existence if the Supplier has not been in existence for 3 years) prior to the date of the Contract:

i) it has conducted all financial accounting and reporting activities in compliance in all material respects with the generally accepted accounting principles that apply to it in any country where it files accounts;

ii) it has been in full compliance with all applicable securities and tax laws and regulations in the jurisdiction in which it is established; and

iii) it has not done or omitted to do anything which could have a material adverse effect on its assets, financial condition or position as an ongoing business concern or its ability to fulfil its obligations under the Contract;

(j) it has and will continue to hold all necessary (if any) regulatory approvals from the Regulatory Bodies necessary to perform its obligations under the Contract; and

(k) 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.

G2.2 The Supplier confirms that in entering into the Contract it is not relying on any statements, warranties or representations given or made (whether negligently or innocently or whether express or implied), or any acts or omissions by or on behalf of the Authority in connection with the subject matter of the Contract except those expressly set out in the Contract and the Supplier hereby waives and releases the Authority in respect thereof absolutely.

G3 Tax Compliance

G3.1 If, during the Term, an Occasion of Tax Non-Compliance occurs, the Supplier shall:

(a) notify the Authority in writing of such fact within 5 Working Days of its occurrence; and

(b) promptly give the Authority:

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

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

G3.2 If the Supplier or any Staff are liable to be taxed in the UK or to pay NICs in respect of consideration received under the Contract, the Supplier shall:

(a) at all times comply with ITEPA and all other statutes and regulations relating to income tax, and SSCBA and all other statutes and regulations relating to NICs, in respect of that consideration; and

(b) indemnify the Authority against any income tax, NICs 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 Staff.

H DEFAULT, DISRUPTION AND TERMINATION

H1 Insolvency and Change of Control

H1.1 The Authority may terminate the Contract with immediate effect by notice and without compensation to the Supplier if the Supplier is a company and in respect of the Supplier:

(a) a proposal is made for a voluntary arrangement within Part I of the Insolvency Act 1986 or of any other composition scheme or arrangement with, or assignment for the benefit of, its creditors;

(b) a shareholders' meeting is convened for the purpose of considering a resolution that it be wound up or a resolution for its winding-up is passed (other than as part of, and exclusively for the purpose of, a bona fide reconstruction or amalgamation);

(c) a petition is presented for its winding up (which is not dismissed within 14 days of its service) or an application is made for the appointment of a provisional liquidator

(d) a receiver, administrative receiver or similar officer is appointed over the whole or any part of its business or assets;

(e) an application order is made either for the appointment of an administrator or for an administration order, an administrator is appointed, or notice of intention to appoint an administrator is given;

(f) it is or becomes insolvent within the meaning of section 123 of the Insolvency Act 1986; or

(g) any event similar to those listed in H1.1 (a)-(f) occurs under the law of any other jurisdiction.

H1.2 The Authority may terminate the Contract with immediate effect by notice and without compensation to the Supplier if the Supplier is an individual and:

(a) an application for an interim order is made pursuant to sections 252-253 of the Insolvency Act 1986 or a proposal is made for any composition scheme or arrangement with, or assignment for the benefit of, the Supplier's creditors;

(b) a petition is presented and not dismissed within 14 days or order made for the Supplier's bankruptcy;

(c) a receiver, or similar officer is appointed over the whole or any part of the Supplier's assets or a person becomes entitled to appoint a receiver, or similar officer over the whole or any part of his assets;

(d) he is unable to pay his debts or has no reasonable prospect of doing so, in either case within the meaning of section 268 of the Insolvency Act 1986;

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

(f) he dies or is adjudged incapable of managing his affairs within the meaning of section 2 of the Mental Capacity Act 2005;

(g) he suspends or ceases, or threatens to suspend or cease, to carry on all or a substantial part of his business; or

(h) any event similar to those listed in clauses H1.2(a) to (g) occurs under the law of any other jurisdiction.

H1.3 The Supplier shall notify the Authority immediately following a merger, take-over, change of control, change of name or status including where the Supplier undergoes a change of control within the meaning of section 1124 of the Corporation Tax Act 2010 (**"Change of Control"**). The Authority may terminate the Contract with immediate effect by notice and without compensation to the Supplier within 6 Months of:

(a) being notified that a Change of Control has occurred; or

(b) where no notification has been made, the date that the Authority becomes aware of the Change of Control

but is not permitted to terminate where Approval was granted prior to the Change of Control.

H1.4 The Authority may terminate the Contract with immediate effect by notice and without compensation to the Supplier if the Supplier is a partnership and:

(a) a proposal is made for a voluntary arrangement within Article 4 of the Insolvent Partnerships Order 1994 or a proposal is made for any other composition, scheme or arrangement with, or assignment for the benefit of, its creditors; or

(b) a petition is presented for its winding up or for the making of any administration order, or an application is made for the appointment of a provisional liquidator; or

(c) a receiver, or similar officer is appointed over the whole or any part of its assets; or

(d) the partnership is deemed unable to pay its debts within the meaning of section 222 or 223 of the Insolvency Act 1986 as applied and modified by the Insolvent Partnerships Order 1994; or

(e) any of the following occurs in relation to any of its partners:

(i) an application for an interim order is made pursuant to sections 252-253 of the Insolvency Act 1986 or a proposal is made for any composition scheme or arrangement with, or assignment for the benefit of, his creditors;

(ii) a petition is presented for his bankruptcy; or

(iii) a receiver, or similar officer is appointed over the whole or any part of his assets;

(f) any event similar to those listed in clauses H1.4 (a) to (e) occurs under the law of any other jurisdiction.

H1.5 The Authority may terminate the Contract with immediate effect by notice and without compensation to the Supplier if the Supplier is a limited liability partnership and:

(a) a proposal is made for a voluntary arrangement within Part I of the Insolvency Act 1986 or a proposal is made for any other composition, scheme or arrangement with, or assignment for the benefit of, its creditors;

(b) an application is made either for the appointment of an administrator or for an administration order, an administrator is appointed, or notice of intention to appoint an administrator is given within Part II of the Insolvency Act 1986;

(c) any step is taken with a view to it being determined that it be wound up (other than as part of, and exclusively for the purpose of, a bona fide reconstruction or amalgamation) within Part IV of the Insolvency Act 1986;

(d) a petition is presented for its winding up (which is not dismissed within 14 days of its service) or an application is made for the appointment of a provisional liquidator within Part IV of the Insolvency Act 1986;

(e) a receiver, or similar officer is appointed over the whole or any part of its assets;

(f) it is or becomes unable to pay its debts within the meaning of section 123 of the Insolvency Act 1986; or

(g) any event similar to those listed in clauses H1.5 (a) to (f) occurs under the law of any other jurisdiction.

H1.6 References to the Insolvency Act 1986 in clause H1.5 (a) are references to that Act as applied under the Limited Liability Partnerships Act 2000 subordinate legislation.

H2 Default

H2.1 The Authority may terminate the Contract with immediate effect by notice if the Supplier commits a Default and:

(a) the Supplier has not remedied the Default to the satisfaction of the Authority within 20 Working Days or such other period as may be specified by the Authority, after issue of a notice specifying the Default and requesting it to be remedied;

(b) the Default is not, in the opinion of the Authority, capable of remedy; or

(c) the Default is a Material Breach.

H2.2 If, through any Default of the Supplier, data transmitted or processed in connection with the Contract is either lost or sufficiently degraded as to be unusable, the Supplier is liable for the cost of reconstitution of that data and shall reimburse the Authority in respect of any charge levied for its transmission and any other costs charged in connection with such Default.

H2.3 If the Authority fails to pay the Supplier undisputed sums of money when due, the Supplier shall give notice to the Authority of its failure to pay. If the Authority fails to pay such undisputed sums within 90 Working Days of the date of such notice, the Supplier may terminate the Contract with immediate effect, save that such right of termination shall not apply where the failure to pay is due to the Authority exercising its rights under clause C2.1 or to a Force Majeure Event.

H3 Termination on Notice

H3.1 The Authority may terminate the Contract at any time by giving 90 days' notice to the Supplier.

H4 Other Grounds

H4.1 The Authority may terminate the Contract if:

(a) the Contract has been subject to a substantial modification which requires a new procurement procedure pursuant to regulation 72(9) of the Regulations;

(b) the Supplier was, at the time the Contract was awarded, in one of the situations specified in regulation 57(1) of the Regulations, including as a result of the application of regulation 57(2), and should therefore have been excluded from the procurement procedure which resulted in its award of the Contract; or

(c) the Supplier has not, in performing the Services, complied with its legal obligations in respect of environmental, social or labour law.

H5 Consequences of Expiry or Termination

H5.1 If the Authority terminates the Contract under clause H2 and makes other arrangements for the supply of the Services the Authority may recover from the Supplier the cost reasonably incurred of making those other arrangements and any additional expenditure incurred by the Authority throughout the remainder of the Term.

H5.2 If the Contract is terminated under clause H2 the Authority shall make no further payments to the Supplier (for Services supplied by the Supplier prior to termination and in accordance with the Contract but where the payment has yet to be made by the Authority), until the Authority has established the final cost of making the other arrangements envisaged under this clause H5.

H5.3 If the Authority terminates the Contract under clauses H3 or H4 the Authority shall make no further payments to the Supplier except for Services supplied by the Supplier prior to termination and in accordance with the Contract but where the payment has yet to be made by the Authority.

H5.4 Save as otherwise expressly provided in the Contract:

(a) termination or expiry of the Contract shall be without prejudice to any rights, remedies or obligations accrued under the Contract prior to termination or

expiration and nothing in the Contract prejudices the right of either Party to recover any amount outstanding at such termination or expiry; and

(b) termination of the Contract does not affect the continuing rights, remedies or obligations of the Authority or the Supplier under clauses C2 (Payment and VAT), C3 (Recovery of Sums Due), D2 (Data Protection and Privacy), D3 (Official Secrets Acts and Finance Act), D4 (Confidential Information), D5 (Freedom of Information), E1 (Intellectual Property Rights), F5 (Audit), G1 (Liability, Indemnity and Insurance), H5 (Consequences of Expiry or Termination), H7 (Recovery), H8 (Retendering and Handover), H9 (Exit Management), H10 (Knowledge Retention), I6 (Remedies Cumulative), I12 (Governing Law and Jurisdiction) and paragraph 9 of Schedule 8.

H6 Disruption

H6.1 The Supplier shall take reasonable care to ensure that in the performance of its obligations under the Contract it does not disrupt the operations of the Authority, its employees or any other contractor employed by the Authority.

H6.2 The Supplier shall immediately inform the Authority of any actual or potential industrial action, whether such action be by its own employees or others, which affects or might affect its ability at any time to perform its obligations under the Contract.

H6.3 If there is industrial action by Staff, the Supplier shall seek Approval for its proposals to continue to perform its obligations under the Contract.

H6.4 If the Supplier's proposals referred to in clause H6.3 are considered insufficient or unacceptable by the Authority acting reasonably, the Contract may be terminated with immediate effect by the Authority.

H6.5 If the Supplier is unable to deliver the Services owing to disruption of the Authority's normal business, the Supplier may request a reasonable allowance of time, and, in addition, the Authority will reimburse any additional expense reasonably incurred by the Supplier as a direct result of such disruption.

H7 Recovery

H7.1 On termination of the Contract for any reason, the Supplier shall at its cost:

(a) immediately return to the Authority all Confidential Information, Personal Data and IP Materials in its possession or in the possession or under the control of any permitted suppliers or Sub-Contractors, which was obtained or produced in the course of providing the Services;

(b) immediately deliver to the Authority all Property (including materials, documents, information and access keys) provided to the Supplier in good working order;

(c) immediately vacate any Authority Premises occupied by the Supplier;

(d) assist and co-operate with the Authority to ensure an orderly transition of the provision of the Services to the Replacement Supplier and/or the completion of any work in progress; and

(e) promptly provide all information concerning the provision of the Services which may reasonably be requested by the Authority for the purposes of adequately understanding the manner in which the Services have been provided and/or for the purpose of allowing the Authority and/or the Replacement Supplier to conduct due diligence.

H7.2 If the Supplier does not comply with clauses H7.1 (a) and (b), the Authority may recover possession thereof and the Supplier grants a licence to the Authority or its appointed agents to enter (for the purposes of such recovery) any premises of the Supplier or its suppliers or Sub-Contractors where any such items may be held.

H8 Retendering and Handover

H8.1 Within 21 days of being requested by the Authority, the Supplier shall provide, and thereafter keep updated, in a fully indexed and catalogued format, all the information necessary to enable the Authority to issue tender documents for the future provision of the Services.

H8.2 The Authority shall take all necessary precautions to ensure that the information referred to in clause H8.1 is given only to potential providers who have qualified to tender for the future provision of the Services.

H8.3 The Authority shall require that all potential providers treat the information in confidence; that they do not communicate it except to such persons within their organisation and to such extent as may be necessary for the purpose of preparing a response to an invitation to tender issued by the Authority; and that they shall not use it for any other purpose.

H8.4 The Supplier indemnifies the Authority against any claim made against the Authority at any time by any person in respect of any liability incurred by the Authority arising from any deficiency or inaccuracy in information which the Supplier is required to provide under clause H8.1.

H8.5 The Supplier shall allow access to the Premises in the presence of an authorised representative, to any person representing any potential provider whom the Authority has selected to tender for the future provision of the Services.

H8.6 If access is required to the Supplier's Premises for the purposes of clause H8.5, the Authority shall give the Supplier 7 days' notice of a proposed visit together with a list showing the names of all persons who will be visiting. Their attendance shall be subject to compliance with the Supplier's security procedures, subject to such compliance not being in conflict with the objectives of the visit.

H8.7 The Supplier shall co-operate fully with the Authority during any handover at the end of the Contract. This co-operation includes allowing full access to both the Authority and the Replacement Supplier, and providing copies of, all documents, reports, summaries and any other information necessary to both the Authority and the Replacement Supplier in order to achieve an effective transition without disruption to routine operational requirements.

H8.8 Within 10 Working Days of being requested by the Authority, the Supplier shall transfer to the Authority, or any person designated by the Authority, free of charge, all computerised filing, recording, documentation, planning and drawing held on software and utilised in the provision of the Services. The transfer shall be made in a fully indexed and catalogued disk format, to operate on a proprietary software package identical to that used by the Authority.

H9 Exit Management

H9.1 On termination of the Contract the Supplier shall render reasonable assistance to the Authority to the extent necessary to effect an orderly assumption by a Replacement Supplier in accordance with the procedure set out in clauses H9.2 to H9.5.

H9.2 If the Authority requires a continuation of all or any of the Services on expiry or termination of the Contract, either by performing them itself or by engaging a third party to perform them, the Supplier shall co-operate fully with the Authority and any such third party and shall take all reasonable steps to ensure the timely and effective transfer of the Services without disruption to routine operational requirements.

H9.3 The following commercial approach shall apply to the transfer of the Services if the Supplier:

(a) does not have to use resources in addition to those normally used to deliver the Services prior to termination or expiry, there shall be no change to the Price; or

(b) reasonably incurs additional costs, the Parties shall agree a Change to the Price based on the Supplier's rates either set out in Schedule 2 or forming the basis for the Price.

H9.4 When requested to do so by the Authority, the Supplier shall deliver to the Authority details of all licences for software used in the provision of the Services including the software licence agreements.

H9.5 Within one Month of receiving the software licence information described in clause H9.4, the Authority shall notify the Supplier of the licences it wishes to be transferred and the Supplier shall provide for the approval of the Authority a plan for licence transfer.

H9.6 Notwithstanding the contents of clauses H9.1-9.5, the Supplier shall comply with the Exit Plan provisions further detailed at Schedule 12.

H10 Knowledge Retention

The Supplier shall co-operate fully with the Authority in order to enable an efficient and detailed knowledge transfer from the Supplier to the Authority on the completion or earlier termination of the Contract and in addition, to minimise any disruption to routine operational requirements. To facilitate this transfer, the Supplier shall provide the Authority free of charge with full access to its Staff, and in addition, copies of all documents, reports, summaries and any other information requested by the Authority.

The Supplier shall comply with the Authority's request for information no later than 15 Working Days from the date that that request was made.

H11 Business Continuity and Disaster

H11. 1 Within sixty 60 days of the Commencement Date, the Supplier shall prepare and deliver to the Authority for the Authority's written approval a plan in line with Schedule 11 Business Continuity and Disaster Recovery, which shall detail the processes and arrangements that the Supplier shall follow to:

H11.1.1 ensure continuity of the business processes and operations supported by the Services following any failure or disruption of any element of the deliverables; and

H11. 1.2 the recovery of the deliverables in the event of a Disaster ("**BCDR Plan**").

H11. 3 The BCDR Plan shall be divided into three sections:

H11.3.1 Section 1 which shall set out general principles applicable to the BCDR Plan;

H11.3.2 Section 2 which shall relate to business continuity (the "**Business Continuity Plan**"); and

H11.3.3 Section 3 which shall relate to Disaster recovery (the "**Disaster Recovery Plan**").

H11.4 Following receipt of the draft BCDR Plan from the Supplier, the Parties shall use reasonable endeavours to agree the contents of the BCDR Plan. If the Parties are unable to agree the contents of the BCDR Plan within twenty (20) Working Days of its submission, then such Dispute shall be resolved in accordance with the Dispute Resolution Procedure.

GENERAL

I1 Dispute Resolution

I1.1 The Parties shall attempt in good faith to negotiate a settlement to any dispute between them arising out of or in connection with the Contract within 20 Working Days of either Party notifying the other of the dispute and such efforts shall involve the escalation of the dispute to the finance director of the Supplier and the commercial director of the Authority.

I1.2 Nothing in this Dispute Resolution Procedure prevents the Parties seeking from any court of competent jurisdiction an interim order restraining the other Party from doing any act or compelling the other Party to do any act.

I1.3 If the dispute cannot be resolved by the Parties pursuant to clause I1.1 either Party may refer it to mediation pursuant to the procedure set out in clause I1.5.

I1.4 The obligations of the Parties under the Contract shall not cease, or be suspended or delayed by the reference of a dispute to mediation (or arbitration) and the Supplier and the Staff shall comply fully with the requirements of the Contract at all times.

I1.5 The procedure for mediation and consequential provisions relating to mediation are as follows:

(a) a neutral adviser or mediator (the **"Mediator"**) shall be chosen by agreement of the Parties or, if they are unable to agree upon a Mediator within 10 Working Days after a request by one Party to the other or if the Mediator agreed upon is unable or unwilling to act, either Party shall within 10 Working Days from the date of the proposal to appoint a Mediator or within 10 Working Days of notice to either Party that he is unable or unwilling to act, apply to the Centre for Effective Dispute Resolution to appoint a Mediator;

(b) the Parties shall within 10 Working Days of the appointment of the Mediator meet with him in order to agree a programme for the exchange of all relevant information and the structure to be adopted for negotiations. If appropriate, the Parties may at any stage seek assistance from the Centre for Effective Dispute Resolution to provide guidance on a suitable procedure;

(c) unless otherwise agreed, all negotiations connected with the dispute and any settlement agreement relating to it shall be conducted in confidence and without prejudice to the rights of the Parties in any future proceedings;

(d) if the Parties reach agreement on the resolution of the dispute, the agreement shall be recorded in writing and shall be binding on the Parties once it is signed by their duly authorised representatives;

(e) failing agreement, either of the Parties may invite the Mediator to provide a non-binding but informative written opinion. Such an opinion shall be provided on a without prejudice basis and shall not be used in evidence in any proceedings relating to the Contract without the prior written consent of both Parties; and

(f) if the Parties fail to reach agreement within 60 Working Days of the Mediator being appointed, or such longer period as may be agreed by the Parties, then any dispute or difference between them may be referred to the Courts unless the dispute is referred to arbitration pursuant to the procedures set out in clause I1.6.

I1.6 Subject to clause I1.2, the Parties shall not start court proceedings until the procedures set out in clauses I1.1 and I1.3 have been completed save that:

(a) the Authority may at any time before court proceedings are commenced, serve a notice on the Supplier requiring the dispute to be referred to and resolved by arbitration in accordance with clause I1.7;

(b) if the Supplier intends to commence court proceedings, it shall serve notice on the Authority of its intentions and the Authority has 21 days following receipt of such notice to serve a reply on the Supplier requiring the dispute to be referred to and resolved by arbitration in accordance with clause I1.7; and

(c) the Supplier may request by notice to the Authority that any dispute be referred and resolved by arbitration in accordance with clause I1.7, to which the Authority may consent as it sees fit.

I1.7 If any arbitration proceedings are commenced pursuant to clause I1.6:

(a) the arbitration is governed by the Arbitration Act 1996 and the Authority shall give a notice of arbitration to the Supplier (the "**Arbitration Notice**") stating:

(i) that the dispute is referred to arbitration; and

(ii) providing details of the issues to be resolved;

(b) the London Court of International Arbitration (**"LCIA"**) procedural rules in force at the date that the dispute was referred to arbitration in accordance with I1.7 (b) shall be applied and are deemed to be incorporated by reference to the Contract and the decision of the arbitrator is binding on the Parties in the absence of any material failure to comply with such rules;

(c) the tribunal shall consist of a sole arbitrator to be agreed by the Parties;

(d) if the Parties fail to agree the appointment of the arbitrator within 10 days of the Arbitration Notice being issued by the Authority under clause I1.7 (a) or if the person appointed is unable or unwilling to act, the arbitrator shall be appointed by the LCIA;

(e) the arbitration proceedings shall take place in London and in the English language; and

(f) the arbitration proceedings shall be governed by, and interpreted in accordance with, English Law.

I2 Force Majeure

I2.1 Subject to this clause I2, a Party may claim relief under this clause I2 from liability for failure to meet its obligations under the Contract 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 the Contract which results from a failure or delay by an agent, Sub-Contractor or supplier is 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.

I2.2 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.

I2.3 If the Supplier is the Affected Party, it is not entitled to claim relief under this clause I2 to the extent that consequences of the relevant Force Majeure Event:

(a) are capable of being mitigated by any of the Services, but the Supplier has failed to do so; and/or

(b) should have been foreseen and prevented or avoided by a prudent provider of services similar to the Services, operating to the standards required by the Contract.

I2.4 Subject to clause I2.5, 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.

I2.5 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.

I2.6 If, as a result of a Force Majeure Event:

(a) an Affected Party fails to perform its obligations in accordance with the Contract, then during the continuance of the Force Majeure Event:

i) the other Party is not entitled to exercise its rights to terminate the Contract in whole or in part as a result of such failure pursuant to clause H2.1 or H2.3; and

ii) neither Party is liable for any Default arising as a result of such failure;

(b) the Supplier fails to perform its obligations in accordance with the Contract it is entitled to receive payment of the Price (or a proportional payment of it) only to the extent that the Services (or part of the Services) continue to be performed in accordance with the Contract during the occurrence of the Force Majeure Event.

I2.7 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 the Contract.

I2.8 Relief from liability for the Affected Party under this clause I2 ends as soon as the Force Majeure Event no longer causes the Affected Party to be unable to comply with its obligations under the Contract and is not dependent on the serving of a notice under clause I2.7.

I3 Notices and Communications

I3.1 Subject to clause I3.3, where the Contract states that a notice or communication between the Parties must be “written” or “in writing” it is not valid unless it is made by letter (sent by hand, first class post, recorded delivery or special delivery) or by email or by communication via Bravo.

I3.2 If it is not returned as undelivered a notice served in:

(a) a letter is deemed to have been received 2 Working Days after the day it was sent; and

(b) an email is deemed to have been received 4 hours after the time it was sent provided it was sent on a Working Day

or when the other Party acknowledges receipt, whichever is the earlier.

I3.3 Notices pursuant to clauses I1, I2 or I7 or to terminate the Contract or any part of the Services are valid only if served in a letter by hand, recorded delivery or special delivery.

I3.4 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 the Contract:

(a) For the Authority:

Contact Name: REDACTED Under FOIA Section 40, Personal Information.

Address: Commercial and Contract Management Directorate (CCMD), 10th Floor, 102 Petty France, London, SW1H 9AJ; and

Email: REDACTED Under FOIA Section 40, Personal Information.

(b) For the Supplier:

Contact Name: REDACTED Under FOIA Section 40, Personal Information.

Address: The National Safety & Security Academy, First Avenue, Finningley, Doncaster, DN9 3RH; and

Email: REDACTED Under FOIA Section 40, Personal Information.

I4 Conflicts of Interest

I4.1 The Supplier shall take appropriate steps to ensure that neither the Supplier nor any Staff is placed in a position where, in the reasonable opinion of the Authority, there is or may be an actual conflict, or a potential conflict, between the pecuniary or personal interests of the Supplier and the duties owed to the Authority under the Contract. The Supplier will notify the Authority immediately giving full particulars of any such conflict of interest which may arise.

I4.2 The Authority may terminate the Contract immediately by notice and/or take or require the Supplier to take such other steps it deems necessary if, in the Authority's reasonable opinion, there is or may be an actual conflict, or a potential conflict, between the pecuniary or personal interests of the Supplier and the duties owed to the Authority under the Contract. The actions of the Authority pursuant to this clause I4 shall not prejudice or affect any right of action or remedy which shall have accrued or shall thereafter accrue to the Authority.

I5 Rights of Third Parties

I5.1 Clauses B10.5 and E1.3 confer benefits on persons named in them (together "**Third Party Provisions**" and each person a "**Third Party Beneficiary**") other than the Parties and are intended to be enforceable by Third Party Beneficiaries by virtue of the Contracts (Rights of Third Parties) Act 1999 ("**CRTPA**").

I5.2 Subject to clause I5.1, a person who is not a Party has no right under the CRTPA to enforce the Contract but this does not affect any right or remedy of any person which exists or is available otherwise than pursuant to the CRTPA and does not apply to the Crown.

I5.3 No Third-Party Beneficiary may enforce or take steps to enforce any Third-Party Provision without Approval.

I5.4 Any amendments to the Contract may be made by the Parties without the consent of any Third-Party Beneficiary.

I6 Remedies Cumulative

Except as expressly provided in the Contract all remedies available to either Party for breach of the Contract are cumulative and may be exercised concurrently or separately, and the exercise of any one remedy are not an election of such remedy to the exclusion of other remedies.

I7 Waiver

I7.1 The failure of either Party to insist upon strict performance of any provision of the Contract, or the failure of either Party to exercise, or any delay in exercising, any right or remedy do not constitute a waiver of that right or remedy and do not cause a diminution of the obligations established by the Contract.

I7.2 No waiver is effective unless it is expressly stated to be a waiver and communicated to the other Party in writing in accordance with clause I3 (Notices and Communications).

I7.3 A waiver of any right or remedy arising from a breach of the Contract does not constitute a waiver of any right or remedy arising from any other or subsequent breach of the Contract.

I8 Severability

If any part of the Contract which is not of a fundamental nature is held invalid, illegal or unenforceable for any reason by any court of competent jurisdiction, such part shall be severed and the remainder of the Contract shall continue in full effect as if the Contract had been executed with the invalid, illegal or unenforceable part eliminated.

I9 Entire Agreement

The Contract constitutes the entire agreement between the Parties in respect of the matters dealt with therein. The Contract supersedes all prior negotiations between the Parties and all representations and undertakings made by one Party to the other, whether written or oral, except that this clause shall not exclude liability in respect of any fraudulent misrepresentation.

I10 Change in Law

I10.1 The Supplier is neither relieved of its obligations to supply the Services in accordance with the terms and conditions of the Contract nor entitled to an increase in the Price as the result of:

(a) a General Change in Law; or

(b) a Specific Change in Law where the effect of that Specific Change in Law on the Services is reasonably foreseeable at the Commencement Date.

I10.2 If a Specific Change in Law occurs or will occur during the Term (other than as referred to in clause I10.1(b)), the Supplier shall:

(a) notify the Authority as soon as reasonably practicable of the likely effects of that change, including whether any:

(i) Change is required to the Services, the Price or the Contract; and

(ii) relief from compliance with the Supplier's obligations is required; and

(b) provide the Authority with evidence:

(i) 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; and

(ii) as to how the Specific Change in Law has affected the cost of providing the Services.

I10.3 Any variation in the Price or relief from the Supplier's obligations resulting from a Specific Change in Law (other than as referred to in clause I10.1(b)) shall be implemented in accordance with clause F4.

I11 Counterparts

The Contract may be executed in counterparts, each of which when executed and delivered constitute an original but all counterparts together constitute one and the same instrument.

I12 Governing Law and Jurisdiction

Subject to clause I1 (Dispute Resolution) the Contract, including any matters arising out of or in connection with it, are governed by and interpreted in accordance with English Law and are subject to the jurisdiction of the Courts of England and Wales. The submission to such jurisdiction does not limit the right of the Authority to take

proceedings against the Supplier in any other court of competent jurisdiction, and the taking of proceedings in any other court of competent jurisdiction does not preclude the taking of proceedings in any other jurisdiction whether concurrently or not.

SCHEDULE 1 – SPECIFICATION

1. General

This Schedule 1 sets out the Services provided by the Supplier and provides a description of what each Service entails.

REDACTED Under FOIA Section 23, Information supplied by, or relating to, bodies dealing with security matters

ANNEX 1: HMCTS SITES

REDACTED Under FOIA Section 23, Information supplied by, or relating to, bodies dealing with security matters

ANNEX 2: SSOPs

REDACTED Under FOIA Section 23, Information supplied by, or relating to, bodies dealing with security matters

SCHEDULE 2 – PRICES and INVOICING

REDACTED Under FOIA Section 43, Commercial Interests

SCHEDULE 3 - CHANGE CONTROL

Change Request Form

(For completion by the Party requesting the Change)

Contract Title:	**Party requesting Change:**
Name of Supplier:	
Change Request Number:	**Proposed Change implementation date:**
Full description of requested Change (including proposed changes to wording of the Contract where possible):	
Reasons for requested Change:	
Effect of requested Change	
Assumptions, dependencies, risks and mitigation (if any):	
Change Request Form prepared by (name):	

Signature:
Date of Change Request:

Contract Change Notice ("CCN")

(For completion by the Authority once the Change has been agreed in principle by both Parties. Changes do not become effective until this form has been signed by both Parties.)

Contract Title:		**Change requested by:**	
Name of Supplier:			
Change Number:			
Date on which Change takes effect:			
Contract between: The Secretary of State for Justice and [insert name of Supplier]			
It is agreed that the Contract is amended, in accordance with Regulation 72 of the Public Contracts Regulations 2015, as follows: [Insert details of the variation (including any change to the Price and deliverables/obligations) based on the information provided in the Change Request Form and any subsequent discussions/negotiations, cross referencing the wording of the original Contract, as previously changed (if applicable), where possible] **Where significant changes have been made to the Contract, information previously published on Contracts Finder will be updated.**			
Words and expressions in this CCN shall have the meanings given to them in the Contract. The Contract, including any previous CCNs, shall remain effective and unaltered except as amended by this CCN			
Signed for and on behalf of the Secretary of State for Justice		**Signed for and on behalf of [insert name of Supplier]**	
Signature		**Signature**	
Name		**Name**	
Title		**Title**	
Date		**Date**	

SCHEDULE 4 - COMMERCIALLY SENSITIVE INFORMATION

1 Without prejudice to the Authority's general obligation of confidentiality, the Parties acknowledge that the Authority may have to disclose Information in or relating to the Contract following a Request for Information pursuant to clause D5 (Freedom of Information).

2 In this Schedule 4 the Parties have sought to identify the Supplier's Confidential Information that is genuinely commercially sensitive and the disclosure of which would be contrary to the public interest.

3 Where possible the Parties have sought to identify when any relevant Information will cease to fall into the category of Information to which this Schedule 4 applies.

4 Without prejudice to the Authority's obligation to disclose Information in accordance with the FOIA and the EIR, the Authority will, acting reasonably but in its sole discretion, seek to apply the commercial interests exemption set out in s.43 of the FOIA to the Information listed below.

SUPPLIER'S COMMERCIALLY SENSITIVE INFORMATION	DATE	DURATION OF CONFIDENTIALITY
Pricing Information	30/10/2024	Contract duration

SCHEDULE 5 - SUPPLIER AND THIRD PARTY SOFTWARE

Supplier Software comprises the following:

Software	Supplier (if Affiliate of the Supplier)	Purpose	No. of Licences	Restrictions	No. of copies	Other	To be deposited in escrow?

Third Party Software comprises the following:

Third Party Software	Supplier	Purpose	No. of Licences	Restrictions	No. of copies	Other	To be deposited in escrow?

SCHEDULE 6 – INFORMATION SECURITY AND ASSURANCE

1.1 This Schedule 6 sets out:

(a) the arrangements the Supplier must implement before, and comply with when, providing the Services and performing its other obligations under the Contract to ensure the security of the Authority Data and the Information Management System;

(b) the Certification Requirements applicable to the Supplier and each of those Sub-contractors which Processes Authority Data;

(c) the security requirements in annex 1, with which the Supplier must comply;

(d) the tests which the Supplier shall conduct on the Information Management System during the Term; and

(e) the Supplier's obligations to:

(i) return or destroy Authority Data on the expiry or earlier termination of the Contract; and

(ii) prevent the introduction of Malicious Software into the Supplier System and to scan for, contain the spread of, and minimise the impact of Malicious Software which is introduced into the Supplier System in paragraph 9; and

(iii) report Breaches of Security to the Authority.

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:

(a) the Premises;

(b) the ICT Environment;

(c) the Information Management System; and

(d) the Services.

2.2 Notwithstanding the involvement of the Authority in assessing the arrangements which the Supplier implements to ensure the security of the Authority Data and the Information Management System, the Supplier is and remains responsible for:

(a) 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; and

(b) the security of the Information Management System.

2.3 The Supplier shall:

(a) comply with the security requirements in annex 1; and

(b) ensure that each Sub-Contractor that Processes Authority Data complies with the Sub-Contractor Security Requirements.

2.4 The Supplier shall provide the Authority with access to Staff responsible for information assurance to facilitate the Authority's assessment of the Supplier's compliance with its obligations set out in this Schedule 6 at reasonable times on reasonable notice.

3 Information Security Approval Statement

3.1 The Supplier shall ensure that its Implementation Plan sets out in sufficient detail how it will ensure compliance with the requirements of this Schedule 6, including any requirements imposed on Sub-Contractors by annex 2, from the Commencement Date.

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

(a) the Supplier has procured the conduct of an IT Health Check of the Supplier System by a CHECK Service Provider or a CREST Service Provider in accordance with paragraph 7.1; and

(b) the Authority has issued the Supplier with an Information Security Approval Statement in accordance with the process set out in this paragraph 3.

3.3 The Supplier shall document in the Security Management Plan how the Supplier and its Sub-Contractors shall comply with the requirements set out in this Schedule and the Contract in order to ensure the security of the Authority Data and the Information Management System.

3.4 The Supplier shall prepare and submit to the Authority within 20 Working Days of the Commencement Date, the Security Management Plan, which comprises:

(a) an Information Assurance Assessment;

(b) the Required Changes Register; and

(c) the Incident Management Process.

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

(a) an Information Security Approval Statement, which shall confirm that the Supplier may use the Information Management System to Process Authority Data; or

(b) a rejection notice, which shall set out the Authority's reasons for rejecting the Security Management Plan.

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

3.7 The Authority may require, and the Supplier shall provide the Authority and its authorised representatives with:

(a) access to the Staff;

(b) access to the Information Management System to audit the Supplier and its Sub-contractors' compliance with the Contract; and

(c) such other information and/or documentation that the Authority or its authorised representatives may reasonably require,

to assist the Authority to establish whether the arrangements which the Supplier and its Sub-Contractors have implemented in order to ensure the security of the Authority Data and the Information Management System are consistent with the representations in the Security Management Plan. The Supplier shall provide the access required by the Authority in accordance with this paragraph 3 within 10 Working Days of receipt of such request, except in the case of a Breach of Security in which case the Supplier shall provide the Authority with the access that it requires within 24 hours of receipt of such request.

4 Compliance Reviews

4.1 The Supplier shall regularly review and update the Security Management Plan, and provide such to the Authority, at least once each year and as required by this paragraph 4.

4.2 The Supplier shall notify the Authority within 2 Working Days after becoming aware of:

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

(b) a new risk to the components or architecture of the Information Management System;

(c) a vulnerability to the components or architecture of the Service which is classified 'Medium', 'High', 'Critical' or 'Important' in accordance with the classification methodology set out in paragraph The severity of vulnerabilities for 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 Security

Management Plan and using the appropriate vulnerability scoring systems including: of annex 1 to this Schedule 6;

(d) a change in the threat profile;

(e) a significant change to any risk component;

(f) a significant change in the quantity of Personal Data held within the Service;

(g) a proposal to change any of the Premises; and/or

(h) an ISO/IEC 27001 (at least ISO/IEC 27001:2013) audit report produced in connection with the Certification Requirements indicates significant concerns.

4.3 Within 10 Working Days of notifying the Authority or such other timescale as may be agreed with the Authority, the Supplier shall make the necessary changes to the Required Changes Register and submit the updated Required Changes Register the Authority for review and approval.

4.4 Where the Supplier is required to implement a change, including any change to the Information Management System, the Supplier shall effect such change at its own cost.

5 Certification Requirements

5.1 The Supplier shall be certified compliant with:

(a) the prevailing version of ISO/IEC 27001 by a UK Accreditation Service-approved certification body or is included within the scope of an existing certification of compliance with ISO/IEC 27001 (at least ISO/IEC 27001:2013); and

(b) Cyber Essentials PLUS

and shall provide the Authority with a copy of each such certificate of compliance before the Supplier is permitted to receive, store or Process Authority Data.

5.2 The Supplier shall ensure that each Higher Risk Sub-contractor is certified compliant with either:

(a) the prevailing version of ISO/IEC 27001 by a UK Accreditation Service-approved certification body or is included within the scope of an existing certification of compliance with ISO/IEC 27001 (at least ISO/IEC 27001:2013); or

(b) Cyber Essentials PLUS

and must provide the Authority with a copy of each such certificate of compliance before the Higher-Risk Sub-contractor is permitted to receive, store or Process Authority Data.

5.3 The Supplier shall ensure that each Medium Risk Sub-contractor is certified compliant with Cyber Essentials.

5.4 The Supplier shall ensure that the Supplier and each Sub-Contractor who is responsible for the secure destruction of Authority Data:

(a) securely destroys Authority Data only at Premises which are included within the scope of an existing certification of compliance with the prevailing published ISO/IEC 27001;

(b) satisfies the Authority that their data destruction/deletion practices comply with UK GDPR and follows all relevant NCSC guidance; and

(c) maintains an asset register of all Authority supplied information, data and equipment to ensure Authority assets are returned and/or deleted.

5.5 The Supplier shall provide the Authority with evidence of its and Sub-Contractors' compliance with the requirements set out in this paragraph 6 before the Supplier or the relevant Sub-Contractor (as applicable) may carry out the secure destruction of any Authority Data.

5.6 The Supplier shall notify the Authority as soon as reasonably practicable and, in any event within 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:

(a) immediately cease using the Authority Data; and

(b) procure that the relevant Sub-Contractor promptly returns, destroys and/or erases the Authority Data in accordance with the requirements set out in this paragraph 5.

5.7 The Authority may exempt, in whole or part, the Supplier or any Sub-Contractor from the requirements of this paragraph 5. Any exemption must be in writing to be effective. The Supplier shall include the exemption in the Security Management Plan.

6 Security Testing

6.1 The Supplier shall, at its own cost procure and conduct:

(a) testing of the Information Management System by a CHECK Service Provider or a CREST Service Provider ("**IT Health Check**"); and

(b) such other security tests as may be required by the Authority.

6.2 The Supplier shall:

(a) complete all of the above security tests before:

(i) the Supplier submits the Security Management Plan to the Authority for review in accordance with paragraph 3; and

(ii) before the Supplier is given permission by the Authority to Process or manage any Authority Data

(b) repeat the IT Health Check not less than once every 12 Months during the Term and submit the results of each such test to the Authority for review in accordance with this paragraph 6.

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

(a) agree with the Authority the aim and scope of the IT Health Check;

(b) promptly, and no later than 10 Working Days, following the receipt of each IT Health Check report, provide the Authority with a copy of the full report;

(c) if the IT Health Check report identifies any vulnerabilities, the Supplier shall:

(i) prepare a remedial plan for approval by the Authority (each a "**Remediation Plan**") which sets out in respect of each vulnerability identified in the IT Health Check report:

(A) how the vulnerability will be remedied;

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

(1) within 3 Months of the date the Supplier received the IT Health Check report in the case of any vulnerability categorised with a severity of “medium”;

(2) within one Month of the date the Supplier received the IT Health Check report in the case of any vulnerability categorised with a severity of “high”; and

(3) within 7 Working Days of the date the Supplier received the IT Health Check report in the case of any vulnerability categorised with a severity of “critical”;

(C) 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;

(ii) comply with the Remediation Plan; and

(iii) conduct such further tests on the Service as are required by the Remediation Plan to confirm that the Remediation Plan has been complied with.

6.4 The Supplier shall ensure that any testing which could adversely affect the Supplier System shall be designed and implemented by the Supplier so as to minimise the

impact on the delivery of the Services and the date, timing, content and conduct of such tests shall be agreed in advance with the Authority.

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

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

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

6.6 The Supplier shall conduct such further tests of the Supplier System as may be required by the Authority from time to time to demonstrate compliance with its obligations set out this Schedule 6 and the Contract.

6.7 The Supplier shall notify the Authority immediately if it fails to, or believes that it will not, mitigate the vulnerability within the timescales set out in paragraph 6.3.

7 Security Monitoring and Reporting

7.1 The Supplier shall:

(a) monitor the delivery of assurance activities;

(b) maintain and update the Security Management Plan in accordance with paragraph 4;

(c) agree a document which presents the residual security risks to inform the Authority's decision to Approve the Supplier to Process and transit the Authority Data;

(d) monitor security risk impacting upon the operation of the Service;

(e) report Breaches of Security in accordance with the approved Incident Management Process; and

(f) agree with the Authority the frequency and nature of the security reports to be prepared and submitted by the Supplier to the Authority within 20 Working Days of the Commencement Date.

8 Malicious Software

8.1 The Supplier shall install and maintain Anti-Malicious Software or procure that 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.

8.2 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 Services to their desired operating efficiency.

8.3 Any cost arising out of the actions of the Parties taken in compliance with paragraph 8.2 shall be borne by the Parties as follows:

(a) by the Supplier where the Malicious Software originates from:

(i) the Supplier Software;

(ii) the Third Party Software supplied by the Supplier; or

(iii) the Authority Data whilst the Authority Data is or was under the control of the Supplier

(i) unless, in the case of the Authority Data only, the Supplier can demonstrate that such Malicious Software was present in the Authority Data and not quarantined or otherwise identified by the Authority when the Authority provided the Authority Data to the Supplier; and

(b) by the Authority, in any other circumstance.

9 Breach of Security

9.1 If either Party becomes aware of a Breach of Security it must notify the other in accordance with the Incident Management Process.

9.2 The Incident Management Process must, as a minimum, require the Supplier to do the following when it becomes aware of a Breach of Security or attempted Breach of Security:

(a) immediately take all reasonable steps necessary to:

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

(ii) remedy such Breach of Security to the extent possible;

(iii) apply a tested mitigation against any such Breach of Security; and

(iv) prevent a further Breach of Security in the future which exploits the same root cause failure;

(b) as soon as reasonably practicable and, in any event, within 2 Working Days, 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.

9.3 If any action is taken in response to a Breach of Security or attempted Breach of Security as a result of non-compliance by the Supplier, its Sub-contractors and/or all or any part of the Information Management System with the Contract, then such remedial action must be completed at no additional cost to the Authority.

ANNEX 1: SECURITY REQUIREMENTS

1 Security Classification of Information

1.1 If the provision of the Services requires the Supplier to Process Authority Data which is classified as:

(a) 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; and/or

(b) SECRET or TOP SECRET, the Supplier shall only do so where it has notified the Authority prior to receipt of such Authority Data and the Supplier shall implement 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.

2 End User Devices

2.1 The Supplier shall manage, and shall ensure that all Sub-Contractors manage, all end-user devices used by the Supplier on which Authority Data is Processed in accordance the following requirements:

(a) the operating system and any applications that Process or have access to Authority Data must be in current support by the vendor, or the relevant community in the case of Open Source operating systems or applications;

(b) users must authenticate before gaining access;

(c) all Authority Data is encrypted using an encryption tool agreed by the Authority;

(d) the end-user device must lock and require any user to re-authenticate after a period of time that is proportionate to the risk environment, during which the end-user device is inactive;

(e) the end-user device must be managed in a way that allows for the application of technical policies and controls over applications that have access to Authority Data;

(f) the Suppler or Sub-Contractor, as applicable, can, without physical access to the end-user device, remove or make inaccessible all Authority Data on the device and prevent any user or group of users from accessing the device;

(g) all end-user devices are within in the scope of any current Cyber Essentials Plus certificate held by the Supplier, or any prevailing ISO/IEC 27001 certification issued by a UKAS-approved certification body, where the scope of that certification includes the Services.

2.2 The Supplier shall comply, and ensure that all Sub-Contractors comply, with the recommendations in NCSC Device Guidance and prevailing Authority Technical Security Guidance, as updated, amended or replaced from time to time, as if those recommendations were incorporated as specific obligations under the Contract.

2.3 Where there any conflict between the requirements of this **Error! Reference source not found.** and the requirements of the NCSC Device Guidance and/or the Authority's Technical Security Guidance, the requirements of this Schedule 6 takes precedence.

3 Encryption

3.1 The Supplier shall ensure, and shall ensure that all Sub-contractors ensure, that Authority Data is encrypted:

(a) when stored at any time when no operation is being performed on it; and

(b) when transmitted.

3.2 Where the Supplier, or a Sub-Contractor, cannot encrypt Authority Data the Supplier shall:

(a) immediately inform the Authority of the subset or subsets of Authority Data it cannot encrypt and the circumstances in which and the reasons why it cannot do so;

(b) provide details of the protective measures the Supplier or Sub-Contractor (as applicable) proposes to take to provide equivalent protection to the Authority as encryption; and

(c) provide the Authority with such information relating to the Authority Data concerned, the reasons why that Authority Data cannot be encrypted and the proposed protective measures as the Authority may require.

3.3 The Authority, the Supplier and, where the Authority requires, any relevant Sub-Contractor shall meet to agree appropriate protective measures for the unencrypted Authority Data.

3.4 Where the Authority and Supplier reach agreement, the Supplier must update the Security Management Plan to include:

(a) the subset or subsets of Authority Data not encrypted and the circumstances in which that will occur; and

(b) the protective measure that the Supplier and/or Sub-contractor will put in please in respect of the unencrypted Authority Data.

3.5 Where the Authority and Supplier do not reach agreement within 40 Working Days of the date on which the Supplier first notified the Authority that it could not encrypt certain Authority Data, either Party may refer the matter to be determined in accordance with the Dispute Resolution Procedure set out in clause I1.

4 Personnel Security

4.1 All Staff are subject to a pre-employment check before they may participate in the provision and or management of the Services which must include all pre-employment checks which are required by the BPSS including: verification of the individual's identity; verification of the individual's nationality and immigration status; verification of the individual's employment history; and verification of the individual's criminal record.

4.2 The Parties shall review the roles and responsibilities of the Staff 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 (for example a Counter Terrorist Check). Roles which are likely to require additional vetting and a specific national security vetting clearance include system administrators whose role would provide those individuals with privileged access to systems which Process Authority Data or data which, if it were Authority Data, would be classified as OFFICIAL-SENSITIVE.

4.3 The Supplier shall not allow Staff who fail the security checks required by paragraphs 4.1 and 4.2 to be involved in the management and/or provision of the Services except where the Authority has expressly agreed in writing to the involvement of the named individual in the management and/or provision of the Services. The Supplier shall provide an up to date list of all Staff and their associated security clearance checks each month, including all Sub-contractor personnel and the personnel of any sub-contractor of a Sub-contractor who in each case are involved in the management and/or provision of the Services.

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

4.5 The Supplier shall ensure that Staff who no longer require access to the Authority Data (for example. 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 Working Day.

4.6 The Supplier shall ensure that Staff who have access to the Premises, the ICT Environment or the Authority Data receive regular training on security awareness that reflects the degree of access those individuals have to the Premises, the ICT Environment or the Authority Data.

4.7 The Supplier shall ensure that the training provided to Staff under paragraph 4.6 includes training on the identification and reporting fraudulent communications intended to induce individuals to disclose Personal Data or any other information that could be used, including in combination with other Personal Data or information, or with other techniques, to facilitate unauthorised access to the Premises, the ICT Environment or the Authority Data (“phishing”).

5 Identity, Authentication and Access Control

5.1 The Supplier shall operate an access control regime to ensure:

(a) all users and administrators of the Supplier System are uniquely identified and authenticated when accessing or administering the Services; and

(b) all persons who access the Premises are identified and authenticated before they are allowed access to the Premises.

5.2 The Supplier shall apply the 'principle of least privilege' when allowing persons access to the Supplier System and Premises so that such persons are allowed access only to those parts of the Premises and the Supplier System they require.

5.3 The Supplier shall retain records of access to the Premises and to the Supplier System and shall make such record available to the Authority on request.

6 Data Destruction or Deletion

6.1 The Supplier shall:

(a) prior to securely sanitising any Authority Data or when requested the Supplier shall provide the Authority with all Authority Data in an agreed open format;

(b) have documented processes to ensure the availability of Authority Data if the Supplier ceases trading;

(c) securely erase in a manner agreed with the Authority any or all Authority Data held by the Supplier when requested to do so by the Authority;

(d) securely destroy in a manner agreed with the Authority all media that has held Authority Data at the end of life of that media in accordance with any specific requirements in the Contract and, in the absence of any such requirements, as agreed by the Authority; and

(e) implement processes which address the NCSC guidance on secure sanitisation.

7 Audit and Protective Monitoring

7.1 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.

7.2 The Parties shall work together to establish any additional audit and monitoring requirements for the Information Management System.

7.3 The Supplier shall discuss with the Authority the retention periods for audit records and event logs which, when agreed with the Authority, shall be documented in the Security Management Plan.

8 Location of Authority Data

8.1 The Supplier shall not and shall procure that none of its Sub-Contractors Process Authority Data outside the UK without Approval.

9 Vulnerabilities and Corrective Action

9.1 The Parties acknowledge that from time to time vulnerabilities in the Information Management System may be discovered which, unless mitigated, will present an unacceptable risk to the Authority Data.

9.2 The severity of vulnerabilities for 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 Security Management Plan and using the appropriate vulnerability scoring systems including:

(a) 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

(b) Microsoft's 'Security Bulletin Severity Rating System' ratings 'Critical', 'Important', and the two remaining levels ('Moderate' and 'Low') respectively.

9.3 Subject to paragraph 9.4, the Supplier shall procure the application of security patches to vulnerabilities in the Information Management System within:

(a) 7 days after the public release of patches for those vulnerabilities categorised as 'Critical';

(b) 30 days after the public release of patches for those vulnerabilities categorised as 'Important'; and

(c) 30 days after the public release of patches for those vulnerabilities categorised as 'Other'.

9.4 The timescales for applying patches to vulnerabilities in the Information Management System set out in paragraph 9.3 shall be extended where:

(a) the Supplier can demonstrate that a vulnerability in the Information Management System is not exploitable within the context of the Services (for example, because it resides in a Software component which is not involved in running in the Services) provided such vulnerabilities shall be remedied by the Supplier within the timescales set out in paragraph 9.3 if the vulnerability becomes exploitable within the context of the Services;

(b) 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 be granted an extension to such timescales of 5 days, provided the Supplier had followed and continues to follow the security patch test plan agreed with the Authority; or

(c) the Authority agrees a different maximum period after a case-by-case consultation with the Supplier under the processes defined in the Security Management Plan.

9.5 The Security Management Plan shall include provisions for major version upgrades of all COTS Software to be kept up to date such that all COTS Software are always in mainstream support throughout the Term unless otherwise agreed by the Authority in

writing. All COTS Software should be no more than N-1 versions behind the latest software release.

10 Secure Architecture

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

(a) 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;

(b) 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

(c) 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:

(i) "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;

(ii) "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;

(iii) "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;

(iv) "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;

(v) "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;

(vi) "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;

(vii) "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;

(viii) "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;

(ix) "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;

(x) "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;

(xi) "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;

(xii) "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;

(xiii) "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; and

(xiv) "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.

(d) the Authority’s Technical Security Guidance

ANNEX 2: SECURITY REQUIREMENTS FOR SUB-CONTRACTORS

1 Application of Annex

1.1 This annex 2 applies to all Sub-Contractors which Process Authority Data.

1.2 The Supplier shall:

(a) ensure that those Sub-Contractors comply with the provisions of this annex 2; and

(b) keep sufficient records to demonstrate that compliance to the Authority.

2 Designing and managing secure solutions

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

2.2 The Sub-Contractor shall assess its systems against the NCSC Cloud Security Principles:

https://www.ncsc.gov.uk/collection/cloud-security?curPage=/collection/cloud-security/implementing-the-cloud-security-principles

at its own cost to demonstrate that the people, process, technical and physical controls have been delivered in an effective way. The Sub-Contractor shall document that assessment and make that documentation available to the Authority on the Authority's request.

3 Data Processing, Storage, Management and Destruction

3.1 The Sub-Contractor shall not Process any Authority Data outside the UK. The Authority may allow the Sub-Contractor to Process Authority Data outside the UK and may impose conditions on that permission, with which the Sub-Contractor shall comply. Any permission must be in writing to be effective.

3.2 The Sub-Contractor shall, when requested to do so by the Authority:

(a) securely destroy Authority Data only on Premises which are included within the scope of an existing certification of compliance with ISO/IEC 27001 or later (at least ISO/IEC 27001:2013);

(b) satisfy the Authority that its data destruction/deletion practices comply with UK GDPR requirements and follows all relevant NCSC guidance; and

(c) maintain an asset register of all Authority supplied information, data and equipment to ensure Authority assets are returned and/or deleted.

4 Personnel Security

4.1 The Sub-Contractor shall perform appropriate checks on their staff before they may participate in the provision and or management of the Services. Those checks must include all pre-employment checks required by the BPSS including: verification of the individual's identity; verification of the individual's nationality and immigration status; verification of the individual's employment history; and verification of the individual's criminal record.

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

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

5 End User Devices

5.1 The Supplier shall manage, and shall ensure that all Sub-contractors manage, all end-user devices used by the Supplier on which Authority Data is Processed in accordance with the following requirements:

(a) the operating system and any applications that Process or have access to Authority Data must be in current support by the vendor, or the relevant community in the case of Open Source operating systems or applications;

(b) users must authenticate before gaining access;

(c) all Authority Data must be encrypted using an encryption tool agreed to by the Authority;

(d) the end-user device must lock and require any user to re-authenticate after a period of time that is proportionate to the risk environment, during which the end-user device is inactive;

(e) the end-user device must be managed in a way that allows for the application of technical policies and controls over applications that have access to Authority Data;

(f) the Suppler or Sub-contractor, as applicable, can, without physical access to the end-user device, remove or make inaccessible all Authority Data on the device and prevent any user or group of users from accessing the device;

(g) all end-user devices are within in the scope of any current Cyber Essentials Plus certificate held by the Supplier, or any ISO/IEC 27001 or later (at least ISO/IEC 27001:2013) certification issued by a UKAS-approved certification body, where the scope of that certification includes the Services.

5.2 The Supplier shall comply, and ensure that all Sub-contractors comply, with the recommendations in NCSC Device Guidance and Authority Technical Security Guidance, as updated, amended or replaced from time to time, as if those recommendations were incorporated as specific obligations under this Agreement.

5.3 Where there any conflict between the requirements of this **Error! Reference source not found.** and the requirements of the NCSC Device Guidance, the requirements of this Schedule 6 takes precedence.

6 Encryption

6.1 The Supplier shall ensure, and shall ensure that all Sub-contractors ensure, that Authority Data is encrypted:

(a) when stored at any time when no operation is being performed on it; and

(b) when transmitted.

6.2 Where the Supplier or a Sub-Contractor cannot encrypt Authority Data the Supplier shall:

(a) immediately inform the Authority of the subset or subsets of Authority Data it cannot encrypt and the circumstances in which and the reasons why it cannot do so;

(b) provide details of the protective measures the Supplier or Sub-Contractor (as applicable) proposes to take to provide equivalent protection to the Authority as encryption; and

(c) provide the Authority with such information relating to the Authority Data concerned, the reasons why that Authority Data cannot be encrypted and the proposed protective measures as the Authority may require.

6.3 The Authority, the Supplier and, where the Authority requires, any relevant Sub-Contractor shall meet to agree appropriate protective measures for the unencrypted Authority Data.

6.4 Where the Authority and Supplier reach agreement, the Supplier shall update the Security Management Plan to include:

(a) the subset or subsets of Authority Data not encrypted and the circumstances in which that will occur; and

(b) the protective measure that the Supplier and/or Sub-Contractor will put in please in respect of the unencrypted Authority Data.

6.5 Where the Authority and Supplier do not reach agreement within 40 Working Days of the date on which the Supplier first notified the Authority that it could not encrypt certain Authority Data, either Party may refer the matter to be determined in accordance with the Dispute Resolution Procedure set out in clause I1.

7 Patching and Vulnerability Scanning

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

8 Third Party Sub-contractors

8.1 The Sub-Contractor shall not transmit or disseminate the Authority Data to any other person unless Approved.

8.2 The Sub-Contractor shall not, when performing any part of the Services, use any software to Process the Authority Data where the licence of that software purports to grant the licensor rights to Process the Authority Data greater than those rights strictly necessary for the use of the software.

ANNEX 3: SECURITY MANAGEMENT PLAN TEMPLATE

Security Management Plan Template

[Project/Service and Supplier Name]

1 Executive Summary

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

2 System Description

2.1 Background

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

2.2 Organisational Ownership/Structure

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

2.3 Information assets and flows

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

2.4 System Architecture

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

2.5 Users

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

2.6 Locations

<Where the data assets are stored and managed from. If any locations hold independent security certifications (e.g. ISO27001 (at least ISO/IEC 27001:2013) these should be noted. Any off-shoring considerations should be detailed.>

2.7 Test and Development Systems

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

2.8 Key roles and responsibilities

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

3 Risk Assessment

3.1 Assurance Scope

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

3.2 Risk appetite

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

3.3 Business impact assessment

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

3.4 Risk assessment

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

Risk ID	Inherent risk	Inherent risk level	Vulnerability	Controls	Residual risk level
R1	Internet attackers could hack the system.	Medium	The service systems are exposed to the internet via the web portal.	C1: Internet-facing firewalls C2: Internet-facing IP whitelist	Very low

Risk ID	Inherent risk	Inherent risk level	Vulnerability	Controls	Residual risk level
				C3: System hardening C4: Protective monitoring C5: Application access control C16: Anti-virus for incoming files C54: Files deleted when processed C59: Removal of departmental identifier	
R2	Remote attackers could intercept or disrupt information crossing the internet.	Medium	File sharing with organisations across the internet.	C9: TLS communications C10: PGP file-sharing	Very low
R3	Internal users could maliciously or accidentally alter bank details.	Medium-High	Users bank details can be altered as part of the normal business function.	C12. System administrators hold SC clearance. C13. All changes to user information are logged and audited. C14. Letters are automatically sent to users' home addresses when bank details are altered.	Low

Risk ID	Inherent risk	Inherent risk level	Vulnerability	Controls	Residual risk level
				C15. Staff awareness training	

3.5 Controls

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

ID	Control title	Control description	Further information and assurance status
C1	Internet-facing firewalls	Internet-facing firewalls are in place between the internet and the system', which restrict access from the internet to the required ports only.	Assured via ITHC firewall rule check
C2	Internet-facing IP whitelist	An IP whitelist is in place for all access from the internet.	Assured via ITHC
C15	Staff awareness training	All staff must undertake annual security awareness training and this process is audited and monitored by line managers.	Assured as part of ISO/IEC 27001 (at least ISO/IEC 27001:2013) certification

3.6 Residual risks and actions

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

4 In-service controls

< This section should describe the controls relating to the information lifecycle, including development, testing, in-service, termination and on-going risk management and accreditation assurance. Details of any formal assurance requirements specified in the contract such as security CHECK testing or maintained ISO/IEC 27001 (at least ISO/IEC 27001:2013) certification should be included. This section should include at least:

(a) information risk management and timescales and triggers for a review;

(b) contractual patching requirements and timescales for the different priorities of patch;

(c) 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;

(d) configuration and change management;

(e) incident management;

(f) vulnerability management;

(g) user access management; and

(h) data sanitisation and disposal.>

5 Security Operating Procedures (SyOPs)

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

6 Major Hardware and Software and end of support dates

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

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

7 Incident Management Process

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

8 Security Requirements for User Organisations

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

9 Required Changes Register

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

Ref	Section	Change	Agreed With	Date agreed	Documentation update	Status

1	6.4	A new Third Party supplier XXXX will be performing the print capability.	Authority name	11/11/2018	Jul-2019	Open

10 Sub-Contractors

<This should include a table which shows for each Sub-contractor their name, the function that they are performing, the data and data volume being processed, the location, and their certification status>

11 Annex A. ISO/IEC 27001 or later (at least ISO/IEC 27001:2013) and/or Cyber Essential Plus certificates

<Any certifications relied upon should have their certificates included>

12 Annex B. Cloud Security Principles assessment

<A spreadsheet may be attached>

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

<A spreadsheet may be attached>

14 Annex D. Latest ITHC report and Remediation Plan

SCHEDULE 7 - PRISONS

ACCESS TO PRISONS

1 If Staff are required to have a pass for admission to an Authority Premises which is a prison, (a "**Prison**") the Authority shall, subject to satisfactory completion of approval procedures, arrange for passes to be issued. Any member of the Staff who cannot produce a proper pass when required to do so by any member of the Authority's personnel, or who contravenes any conditions on the basis of which a pass was issued, may be refused admission to a Prison or be required to leave a Prison if already there.

2 Staff shall promptly return any pass if at any time the Authority so requires or if the person to whom the pass was issued ceases to be involved in the performance of the Services. The Supplier shall promptly return all passes on expiry or termination of the Contract.

3 Staff attending a Prison may be subject to search at any time. Strip searches shall be carried out only on the specific authority of the Authority under the same rules and conditions applying to the Authority's personnel. The Supplier is referred to Rule 71 of Part IV of the Prison Rules 1999 as amended by the Prison (Amendment) Rules 2005 and Rule 75 of Part IV of the Young Offender Institution Rules 2000 as amended by the Young Offender Institution (Amendment) Rules 2005.

4 Searches shall be conducted only on the specific authority of the Authority under the same rules and conditions applying to the Authority's personnel and/or visitors. The Supplier is referred to Section 8 of the Prison Act 1952, Rule 64 of the Prison Rules 1999 and PSI 07/2016.

SECURITY

5 Whilst at Prisons Staff shall comply with all security measures implemented by the Authority in respect of staff and other persons attending Prisons. The Authority shall provide copies of its written security procedures to Staff on request. The Supplier and all Staff are prohibited from taking any photographs at Prisons unless they have Approval and the Authority's representative is present so as to have full control over the subject matter of each photograph to be taken. No such photograph shall be published or otherwise circulated without Approval.

6 The Authority may search vehicles used by the Supplier or Staff at Prisons.

7 The Supplier and Staff shall co-operate with any investigation relating to security which is carried out by the Authority or by any person who is responsible for security matters on the Authority's behalf, and when required by the Authority shall:

7.1 take all reasonable measures to make available for interview by the Authority any members of Staff identified by the Authority, or by a person who is responsible for security matters, for the purposes of the investigation. Staff may be accompanied by and be advised or represented by another person whose attendance at the interview is acceptable to the Authority; and

7.2 subject to any legal restriction on their disclosure, provide all documents, records or other material of any kind and in whatever form which may be reasonably required by the Authority, or by a person who is responsible for security matters on the Authority's behalf, for the purposes of investigation as long as the provision of that material does not prevent the Supplier from performing the Services. The Authority may retain any

such material for use in connection with the investigation and, as far as possible, may provide the Supplier with a copy of any material retained.

OFFENCES AND AUTHORISATION

8 In providing the Services the Supplier shall comply with PSI 10/2012 (Conveyance and Possession of Prohibited Items and Other Related Offences) and other applicable provisions relating to security as published by the Authority from time to time.

9 Nothing in the Contract is deemed to provide any "authorisation" to the Supplier in respect of any provision of the Prison Act 1952, Offender Management Act 2007, Crime and Security Act 2010, Serious Crime Act 2015 or other relevant legislation.

SCHEDULE 8 – STATUTORY OBLIGATIONS AND CORPORATE SOCIAL RESPONSIBILITY

1 What the Authority expects from the Supplier

1.1 Her Majesty's Government's Supplier Code of Conduct (the "**Code**") sets out the standards and behaviours expected of suppliers who work with government. The Code can be found online at:

Supplier Code of Conduct - v2 (publishing.service.gov.uk)

1.2 The Supplier shall, and shall procure that its Sub-Contractors shall:

1.2.1 comply with its legal obligations, in particular those in Part 1 of this Schedule 8, and meet the standards set out in the Code as a minimum; and

1.2.2 use reasonable endeavours to comply with the standards in Part 2 of this Schedule 8.

PART 1 Statutory Obligations

2 Equality and Accessibility

2.1 The Supplier shall:

(a) perform its obligations under the Contract in accordance with:

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

ii) the Authority's equality, diversity and inclusion policy as given to the Supplier from time to time; and

iii) any other requirements and instructions which the Authority reasonably imposes regarding any equality obligations imposed on the Authority at any time under applicable equality law

(b) 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).

3 Modern Slavery

3.1 The Supplier shall:

(a) not use, or allow Sub-Contractors to use, forced, bonded or involuntary prison labour;

(b) not require any Staff to lodge deposits or identity papers with their employer;

(c) allow, and ensure that any Sub-Contractors allow, Staff to leave their employer after reasonable notice;

(d) make reasonable enquiries to ensure that its Staff and Sub-Contractors have not been convicted of slavery or human trafficking offences anywhere in the world;

(e) have and maintain throughout the Term its own policies and procedures to ensure its compliance with the MSA and include in its Sub-Contracts anti-slavery and human trafficking provisions;

(f) not use, or allow its Staff to use physical abuse or discipline, the threat of physical abuse, sexual or other harassment and verbal abuse or other forms of intimidation of its Staff and Sub-Contractors;

(g) not use or allow to be used child or slave labour to be used by its Sub-Contractors;

(h) if either Party identifies any occurrence of modern slavery in connection with the Contract, comply with the rectification process set out in clauses F2.4 to F2.6;

(i) prepare and deliver to the Authority each year, an annual slavery and trafficking report setting out the steps it has taken to ensure that slavery and trafficking is not taking place in any of its supply chains or in any part of its business;

(j) maintain a complete set of records to trace the supply chain of all Services provided to the Authority in connection with the Contract;

(k) report the discovery or suspicion of any slavery or trafficking by it or its Sub-Contractors to the Authority and to the Modern Slavery Helpline and other relevant national or local law enforcement agencies; and

(l) implement a system of training for its employees to ensure compliance with the MSA.

3.2 The Supplier represents, warrants and undertakes throughout the Term that:

(a) it has not been convicted of any slavery or human trafficking offences anywhere in the world; and

(b) to the best of its knowledge it is not currently under investigation, inquiry or enforcement proceedings in relation to any allegation of slavery or human trafficking offences anywhere in the world.

3.3 If the Supplier notifies the Authority pursuant to paragraph 3.1(i) of this Schedule 8, it 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 the Contract.

3.4 If the Supplier is in Default under paragraphs 3.1 or 3.2 of this Schedule 8 the Authority may by notice:

(a) require the Supplier to remove from performance of the Contract any Sub-Contractor, Staff or other persons associated with it whose acts or omissions have caused the Default; or

(b) immediately terminate the Contract.

4 Income Security

4.1 The Supplier shall:

(a) ensure that all pay and benefits paid for a standard working week meet, at least, national legal standards in the country of employment;

(b) provide all Staff with written and readily understandable information about their employment conditions in respect of pay before they enter employment and about their pay for the pay period concerned each time that they are paid;

(c) not make deductions from pay:

(i) as a disciplinary measure;

(ii) except where permitted by Law and the terms of the employment contract; and

(iii) without express permission of the person concerned

(d) record all disciplinary measures taken against Staff.

5 Working Hours

5.1 The Supplier shall ensure that:

(a) the working hours of Staff comply with the Law, and any collective agreements;

(b) the working hours of Staff, excluding overtime, is defined by contract, do not exceed 48 hours per week unless the individual has agreed in writing, and that any such agreement is in accordance with the Law;

(c) overtime is used responsibly, considering:

(i) the extent;

(ii) frequency; and

(iii) hours worked;

(d) the total hours worked in any seven-day period shall not exceed 60 hours, except where covered by paragraph 5.1 (e);

(e) working hours do not exceed 60 hours in any seven-day period unless:

(i) it is allowed by Law;

(ii) it is allowed by a collective agreement freely negotiated with a worker's organisation representing a significant portion of the workforce;

(iii) appropriate safeguards are taken to protect the workers' health and safety; and

(iv) the Supplier can demonstrate that exceptional circumstances apply such as during unexpected production peaks, accidents or emergencies;

(f) all Supplier Staff are provided with at least:

(i) 1 day off in every 7-day period; or

(ii) where allowed by Law, 2 days off in every 14-day period.

6 Right to Work

6.1 The Supplier shall:

(a) ensure that all Staff, are employed on the condition that they are permitted to work in the UK, and;

(b) notify the authority immediately if an employee is not permitted to work in the UK.

7 Health and Safety

7.1 The Supplier shall perform its obligations under the Contract in accordance with:

(a) all applicable Law regarding health and safety; and

(b) the Authority's Health and Safety Policy while at the Authority's Premises.

7.2 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's Premises of which it becomes aware and which relate to or arise in connection with the performance of the Contract. The Supplier shall instruct Staff to adopt any necessary safety measures in order to manage the risk.

8. Welsh Language Requirements

8.1 The Supplier shall comply with the Welsh Language Act 1993 and the Welsh Language Scheme as if it were the Authority to the extent that the same relate to the provision of the Services.

9 Fraud and Bribery

9.1 The Supplier represents and warrants that neither it, nor to the best of its knowledge any Staff, have at any time prior to the Commencement Date:

(a) 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

(b) 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.

9.2 The Supplier shall not during the Term:

(a) commit a Prohibited Act; and/or

(b) do or suffer anything to be done which would cause the Authority or any of its 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.

9.3 The Supplier shall, during the Term:

(a) 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;

(b) have in place reasonable prevention measures (as defined in section 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;

(c) keep appropriate records of its compliance with its obligations under paragraph 9.3 (a) and 9.3 (b) and make such records available to the Authority on request; and

(d) 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

9.4 The Supplier shall immediately notify the Authority in writing if it becomes aware of any breach of paragraphs 9.1 and/or 9.2, or has reason to believe that it has or any of the Staff have:

(a) been subject to an investigation or prosecution which relates to an alleged Prohibited Act;

(b) 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

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

9.5 If the Supplier notifies the Authority pursuant to paragraph 9.4, 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.

9.6 If the Supplier is in Default under paragraphs 9.1 and/or 9.2, the Authority may by notice:

(a) require the Supplier to remove from performance of the Contract any Staff whose acts or omissions have caused the Default; or

(b) immediately terminate the Contract.

9.7 Any notice served by the Authority under paragraph 9.6 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 taken (including, where relevant, the date on which the Contract terminates).

PART 2 Corporate Social Responsibility

10 Zero Hours Contracts

10.1 Any reference to zero hours contracts, for the purposes of this Contract, means as they relate to employees or workers and not those who are genuinely self-employed and undertaking work on a zero hours arrangement.

10.2 When offering zero hours contracts, the Supplier shall consider and be clear in its communications with its employees and workers about:

(a) whether an individual is an employee or worker and what statutory and other rights they have;

(b) the process by which work will be offered and assurance that they are not obliged to accept work on every occasion; and

(c) how the individual's contract will terminate, for example, at the end of each work task or with notice given by either party.

11 Sustainability

11.1 The Supplier shall:

(a) comply with the applicable Government Buying Standards;

(b) provide, from time to time, in a format reasonably required by the Authority, reports on the environmental effects of providing the Goods and Services;

(c) maintain ISO 14001 or BS 8555 or an equivalent standard intended to manage its environmental responsibilities; and

(b) perform its obligations under the Contract in a way that:

(i) supports the Authority's achievement of the Greening Government Commitments;
(ii) conserves energy, water, wood, paper and other resources;

(iii) reduces waste and avoids the use of ozone depleting substances; and

(iv) minimises the release of greenhouse gases, volatile organic compounds and other substances damaging to health and the environment.

SCHEDULE 9 – DATA PROCESSING

1. The contact details of the Authority's Data Protection Officer are: data.compliance@justice.gov.uk ***or*** Data Protection Officer, 102 Petty France, London, SW1H 9AJ.

The contact details of the Supplier's Data Protection Officer are: REDACTED Under FOIA Section 40, Personal Information.

2.
3. The Supplier shall comply with any further written instructions with respect to Processing by the Authority.

4. Any such further instructions shall be incorporated into this Schedule 9.

Description	**Details**
Subject matter of the processing	*[This should be a high level, short description of what the processing is about i.e. its subject matter of the contract.* *Example: The processing is needed in order to ensure that the Supplier can effectively deliver the contract to provide a service to members of the public]*
Duration of the processing	*[Clearly set out the duration of the processing including dates]*
Nature and purposes of the processing	*[Be as specific as possible, but make sure that you cover all intended purposes. The nature of the processing means any operation such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data (whether or not by automated means) etc.The purpose might include: employment processing, statutory obligation, recruitment assessment etc]*
Type of Personal Data being Processed	*[Examples here include: name, address, date of birth, NI number, telephone number, pay, images, biometric data etc]*
Categories of Data Subject	*[Examples include: Staff (including volunteers, agents, and temporary workers), customers/ clients, suppliers, patients, students / pupils, members of the public, users of a particular website etc]*
International Transfers and legal gateway	*[Explain where geographically personal data may be stored or accessed from. Explain the legal gateway you are relying on to export the data e.g. adequacy decision, EU SCCs, UK IDTA. Annex any SCCs or IDTA to this contract]*

Plan for return and destruction of the data once the processing is complete Unless requirement under union or member state law to preserve that type of data	*[Describe how long the data will be retained for, how it be returned or destroyed]*

SCHEDULE 10 – IMPLEMENTATION PLAN

1 INTRODUCTION

1.1 This Schedule:

(a) defines the process for the preparation and implementation of the Implementation Plan; and

(b) identifies the Milestones (and associated Deliverables).

2 APPROVAL OF THE IMPLEMENTATION PLAN

2.1 The Supplier shall submit a draft of the Implementation Plan to the Authority for approval within 10 Working Days of the Commencement Date.

2.2 The Supplier shall ensure that the draft Implementation Plan:

(a) incorporates all of the Milestones and Milestone Dates;

(b) identifies Milestones which are Key Milestones;

(c) includes (as a minimum) the Supplier's proposed timescales in respect of the following for each of the Key Milestones which are set out below:

(i) BPSS and Counter Terrorist Check (CTC) Clearance for operational staff;

(ii) Competencies of Testers and those administering the system, including evidence of training provided, professional accreditation and experience;

(iii) Secure Cloud-Based Reporting System set-up with the functionality detailed in Schedule 1;

(iv) Copies of the Suppliers Operating Procedures to ensure safe and effective delivery of the tests in line with SSOPs;

(v) Details of the rectification training to be delivered by a Tester to the security officer at an HMCTS Site in the event of a failed test under the Core Services;

(vi) Development of Test Pieces and positioning of Test Pieces during performance of Core Services in accordance with Schedule 1; and

(vii) The format of details to be included in the Assessment Reports and monthly reports as required by Schedule 1.

(d) clearly outlines all the steps required to implement the Milestones to be achieved by the end of the Mobilisation Period, together with a high level plan for the rest of the programme, in conformity with the terms of this Contract;

(e) contains all the necessary information obtained from the previous supplier to ensure a smooth handover from the previous contract and in order for the Supplier to perform its obligations under this Contract; and

(f) clearly outlines the required roles and responsibilities of both Parties, including staffing requirements.

2.3 Prior to the submission of the draft Implementation Plan to the Authority in accordance with Paragraph 2.1, the Authority shall have the right:

(a) to review any documentation produced by the Supplier in relation to the development of the Implementation Plan, including:

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

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

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

(b) to require the Supplier to include any reasonable changes or provisions in the Implementation Plan.

2.4 Following receipt of the draft Implementation Plan from the Supplier, the Authority shall:

(a) review and comment on the draft Implementation Plan as soon as reasonably practicable; and

(b) notify the Supplier in writing that it approves or rejects the draft Implementation Plan no later than 5 Working Days after the date on which the draft Implementation Plan is first delivered to the Authority.

2.5 If the Authority rejects the draft Implementation Plan:

(a) the Authority shall inform the Supplier in writing of its reasons for its rejection; and

(b) the Supplier shall then revise the draft Implementation Plan (taking reasonable account of the Authority's comments) and shall re-submit a revised draft Implementation Plan to the Authority for the Authority's approval within 5 Working Days of the date of the Authority's notice of rejection. The provisions of Paragraph 2.4 and this Paragraph 2.5 2.5 shall apply again to any resubmitted draft Implementation Plan, provided that

either Party may refer any disputed matters for resolution in accordance with Clause I1 at any time.

2.6 If the Authority approves the draft Implementation Plan, it shall be deemed the approved Implementation Plan from the date of the Authority's notice of approval.

3 Not used

4 GOVERNMENT REVIEWS

4.1 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 the costs of such a review shall be borne by the Supplier.

SCHEDULE 11 – Business Continuity and Disaster recovery

1.1 Section 1 OF THE BCDR PLAN - GENERAL PRINCIPLES

1.1.1 set out how the business continuity and Disaster recovery elements of the BCDR Plan link to each other;

1.1.2 provide details of how the invocation of any element of the BCDR Plan may impact upon the provision of the Services provided to the Authority by a Related Supplier;

1.1.3 contain an obligation upon the Supplier to liaise with the Authority and any Related Suppliers with respect to business continuity and Disaster recovery;

1.1.4 detail how the BCDR Plan interoperates with any overarching Disaster recovery or business continuity plan of the Authority and any of its other Related Suppliers in each case as notified to the Supplier by the Authority from time to time;

1.1.5 contain a communication strategy including details of an incident and problem management service and advice and help desk facility which can be accessed via multiple channels;

1.1.6 contain a risk analysis, including:

1.1.6.1 failure or disruption scenarios and assessments of likely frequency of occurrence;

1.1.6.2 identification of any single points of failure within the provision of the Services and processes for managing those risks;

1.1.6.3 identification of risks arising from the interaction of the provision of the Services with the goods and/or services provided by a Related Supplier; and

1.1.6.4 a business impact analysis of different anticipated failures or disruptions;

1.1.7 provide for documentation of processes, including business processes, and procedures;

1.1.8 set out key contact details for the Supplier (and any Subcontractors) and for the Authority;

1.1.9 identify the procedures for reverting to "normal service";

1.1.10 set out method(s) of recovering or updating data collected (or which ought to have been collected) during a failure or disruption to minimise data loss;

1.1.11 identify the responsibilities (if any) that the Authority has agreed it will assume in the event of the invocation of the BCDR Plan; and

1.1.12 provide for the provision of technical assistance to key contacts (including Related Suppliers) at the Authority's Premises as required by the Authority to inform decisions in support of the Authority's business continuity plans.

1.2 The BCDR Plan shall be designed so as to ensure that:

1.2.1.1 the Services are provided in accordance with this Contract at all times during and after the invocation of the BCDR Plan;

1.2.1.2 the adverse impact of any Disaster is minimised as far as reasonably possible;

1.2.2 it complies with the relevant provisions of ISO/IEC 27002; ISO22301/ISO22313 and all other industry standards from time to time in force; and

1.2.3 it details a process for the management of Disaster recovery testing.

1.3 The BCDR Plan shall be upgradeable and sufficiently flexible to support any changes to the Services and the business operations.

1.4 The Supplier shall not be entitled to any relief from its obligations under the KPIs or to any increase in the Price to the extent that a Disaster occurs as a consequence of any breach by the Supplier of this Contract (including any failure by the Supplier to provide the Service).

2 Section 2 OF THE BCDR PLAN - BUSINESS CONTINUITY

2.1 The Business Continuity Plan shall set out the arrangements that are to be invoked to ensure that the business processes remain supported and to ensure continuity of the business operations supported by the Services including:

2.1.1 the alternative processes, options and responsibilities that may be adopted in the event of a failure in or disruption to the provision of the Services; and

2.1.2 the steps to be taken by the Supplier upon resumption of the provision of Services in order to address the effect of the failure or disruption.

2.2 The Business Continuity Plan shall:

2.2.1 address the various possible levels of failures of or disruptions to the Services;

2.2.2 set out the goods and/or Services to be provided and the steps to be taken to remedy the different levels of failures of and disruption to the Services;

2.2.3 specify any applicable KPIs with respect to the provision of the Services that may, as a result of the Business Continuity plan being implemented, be affected and which the Supplier may seek approval from the Authority for the relaxation of the KPIs in respect of the provision of the Services during any period of invocation of the Business Continuity Plan; and

2.2.4 set out the circumstances in which the Business Continuity Plan is invoked.

3 Section 3 OF THE BCDR PLAN - DISASTER RECOVERY

3.1 The Disaster Recovery Plan (which shall be invoked only upon the occurrence of a Disaster) shall be designed to ensure that upon the occurrence of a Disaster the Supplier ensures continuity of the business operations of the Authority supported by the Services following any Disaster or during any period of service failure or disruption with, as far as reasonably possible, minimal adverse impact.

3.2 The Supplier's BCDR Plan shall include an approach to business continuity and Disaster recovery that addresses the following:

3.2.1 loss of access to the Authority’s Premises;

3.2.2 loss of utilities to the Authority’s Premises;

3.2.3 loss of the Supplier's helpdesk or Information Management System;

3.2.4 loss of a Subcontractor;

3.2.5 emergency notification and escalation process;

3.2.6 contact lists;

3.2.7 staff training and awareness;

3.2.8 BCDR Plan testing;

3.2.9 post implementation review process;

3.2.10 any applicable KPI with respect to the provision of the disaster recovery services and Services that may, as a result of the Disaster Recovery Plan being implemented, be affected and which the Supplier may seek approval from the Authority to relax in respect of the provision of other Services during any period of invocation of the Disaster Recovery Plan;

3.2.11 details of how the Supplier shall ensure compliance with security standards ensuring that compliance is maintained for any period during which the Disaster Recovery Plan is invoked;

3.2.12 access controls to any Disaster recovery sites used by the Supplier in relation to its obligations pursuant to this Schedule; and

3.2.13 testing and management arrangements.

4 REVIEW AND AMENDMENT OF THE BCDR PLAN

4.1 The Supplier shall review the BCDR Plan:

4.1.1 on a regular basis and as a minimum once every six (6) Months;

4.1.2 within three (3) Months of the BCDR Plan (or any part) having been invoked pursuant to Paragraph 5; and

4.1.3 where the Authority requests in writing any additional reviews (over and above those provided for in Paragraphs 4.1.1 and 4.1.2 of this Schedule) whereupon the Supplier shall 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.

4.2 Each review of the BCDR Plan pursuant to Paragraph 4.1 shall assess its suitability having regard to any change to the Services or any underlying business processes and operations facilitated by or supported by the Services which have taken place since the later of the original approval of the BCDR Plan or the last review of the BCDR 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 BCDR Plan. The review shall be completed by the Supplier within such period as the Authority shall reasonably require.

4.3 The Supplier shall, within twenty (20) Working Days of the conclusion of each such review of the BCDR Plan, provide to the Authority a report (a **"Review Report"**) setting out the Supplier's proposals (the **"Supplier's Proposals"**) for addressing any changes in the risk profile and its proposals for amendments to the BCDR Plan.

4.4 Following receipt of the Review Report and the Supplier's Proposals, the Parties shall use reasonable endeavours to agree the Review Report and the Supplier's Proposals. If the Parties are unable to agree Review Report and the Supplier's Proposals within twenty (20) Working Days of its submission, then such Dispute shall be resolved in accordance with the Dispute Resolution Procedure.

4.5 The Supplier shall as soon as is reasonably practicable after receiving the approval of the Supplier's Proposals 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 Service.

5 TESTING OF THE BCDR PLAN

5.1 The Supplier shall test the BCDR Plan:

5.1.1 regularly and in any event not less than once in every Contract year;

5.1.2 in the event of any major reconfiguration of the Services; and

5.1.3 at any time where the Authority considers it necessary (acting in its sole discretion).

5.2 If the Authority requires an additional test of the BCDR Plan under paragraph 5.1.3, 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 BCDR Plan. The Supplier's costs of the additional test shall be borne by the Authority unless the BCDR Plan fails the additional test in which case the Supplier's costs of that failed test shall be borne by the Supplier.

5.3 The Supplier shall undertake and manage testing of the BCDR Plan in full consultation with and under the supervision of the Authority and shall liaise with the Authority in respect of the planning, performance, and review, of each test, and shall comply with the reasonable requirements of the Authority

5.4 The Supplier shall ensure that any use by it or any Subcontractor 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.

5.5 The Supplier shall, within twenty (20) Working Days of the conclusion of each test, provide to the Authority a report setting out:

5.5.1 the outcome of the test;

5.5.2 any failures in the BCDR Plan (including the BCDR Plan's procedures) revealed by the test; and

5.5.3 the Supplier's proposals for remedying any such failures.

5.6 Following each test, the Supplier shall take all measures requested by the Authority to remedy any failures in the BCDR Plan and such remedial activity and re-testing shall be completed by the Supplier, at its own cost, by the date reasonably required by the Authority.

6 INVOCATION OF THE BCDR PLAN

6.1 In the event of a complete loss of service or in the event of a Disaster, the Supplier shall immediately invoke the BCDR Plan (and shall inform the Authority promptly of such invocation). In all other instances the Supplier shall invoke or test the BCDR Plan only with the prior consent of the Authority.

6.2 The provisions of this Schedule 11 are without a prejudice to the rights of the Authority.

7 FORCE MAJEURE

7.1 The Supplier will not be entitled to rely on the Force Majeure provisions, if the Supplier would not have been impacted by the Force Majeure event had it complied with the provisions of this Schedule 11 and the BDCR.

SCHEDULE 12 – EXIT MANAGEMENT

1 DEFINITIONS

1.1 In this Schedule, the following definitions shall apply:

"Exit Plan"	means the exit management plan developed by the Supplier and approved by the Authority in accordance with paragraph 1 of this Schedule.

1. EXIT PLAN

1.1 The Supplier shall no later than six months prior to the second anniversary of the Commencement Date, deliver to the Authority an Exit Plan which complies with the requirements set out in paragraph 1.3 of this Schedule and is otherwise reasonably satisfactory to the Authority. Notwithstanding this paragraph 1.1, the Authority may upon reasonable notice require specifics further to that set out at paragraph 1.3 to be provided by the Supplier and included within the Exit Plan.

1.2 NOT USED

1.3 The Authority shall review the Exit Plan and shall either

a) Reject the Exit plan giving reasons or

b) Accept the Exit Plan

1.4 Where the Exit Plan is rejected the Authority shall

a) Give reasonable grounds for its decision and

b) Request the Supplier provides a revised Exit Plan within 14 Working Days

1.5 Only if (by notification to the Supplier in writing) the Authority agrees with a draft Exit Plan provided by the Supplier under paragraph 1.1 shall that draft become the Exit Plan for this Contract.

1.6 The Exit Plan shall set out, as a minimum:

1.6.1 a detailed description of both the transfer and cessation processes, including a timetable;

1.6.2 how the Services will transfer to the Replacement Supplier;

1.6.3 details of any contracts which will be available for transfer to the Replacement Supplier upon the End Date together with any reasonable costs required to effect such transfer;

1.6.4 proposals for the training of key members of the Replacement Supplier's staff in connection with the continuation of the provision of the Services following the End Date;

1.6.5 proposals for providing the Authority or a Replacement Supplier copies of all documentation relating to the use and operation of the Services and required for their continued use;

1.6.6 proposals for the assignment or novation of all services utilised by the Supplier in connection with the supply of the Services;

1.6.7 proposals for the identification and return of all Authority property in the possession of and/or control of the Supplier or any third party;

1.6.8 proposals for the disposal of any redundant deliverables and materials;

1.6.9 any other information or assistance reasonably required by the Authority or a Replacement Supplier; and

1.6.10 be maintained by the Supplier at all times, for the purpose of ensuring that the Exit Plan remains valid and correct during its period of operation. The Supplier shall make such amendments deemed necessary by either Party within a reasonable timeframe and submit these amendments to the Authority for approval.

1.7 A version of an Exit Plan agreed between the parties shall not be superseded by any draft submitted by the Supplier.

1.8 The Supplier is hereby reminded of its obligations in relation to data retention and protection elsewhere in this Contract. The Supplier also recognises that its obligations within this Schedule 12 do not supersede, extinguish or otherwise amend any such obligations.

Execution

Signature page of the Contract between the Secretary of State for Justice and Redline Aviation Security Limited

This Contract is duly executed by the Parties on the date which appears at the head of page 1.

SIGNED for and on behalf of the
Secretary of State for Justice

Signature:

Name (block capitals):

Position:

Date:

SIGNED for and on behalf of the Redline Aviation Security Limited

Signature:

Name (block capitals):

Position:

Date: