Contract part two of two.

APPENDIX C SERVICE LEVELS AND MANAGEMENT REPORTING

C1 Throughout the life of the Agreement the Supplier's contract performance will be measured against identified Key Performance Indicators and specific Service Levels to evidence that the Supplier is fulfilling the Contract requirements.

C2.The Supplier will be required to provide detailed and specific Contract Management Information (MI) to the Authority against identified Key Performance Indicators described within this Appendix, and shall record their levels of service achieved against defined target Service Levels. The supply of accurate information and performance in meeting those Service Levels is deemed material to the performance of the Contract.

C3. The Supplier shall ensure that they are fully capable of gathering data and set up reports at the commencement of the Contract and account set up.

Management Information Reporting Requirements

C4. The supply of Management Information is a requirement of the Agreement to allow the Authority's Operational Contract Manager to track sales and demand and to manage inventory; also to provide assurance of the Supplier's performance against the Contract requirements.

C5. The format of the reporting fields shall be stipulated by the Authority. The Supplier should be aware that Management Information may be requested via email or a request submitted via the MoJ e-Sourcing Portal in the form of Requests for Information (RFI's). The Authority is currently developing its electronic Procurement portfolio and may request that the Supplier takes part in electronic contract monitoring via the e-Sourcing Portal Supplier Performance Management module (SPM).

C6. The method of performance reporting via SPM will be shared with the Supplier and feedback given following requests for information.

C7. The information shall be supplied free of charge to the Authority.

C8. The Supplier is required to structure all ordering locations with suitable identifiers to allow spend information to be split by organisation and location as per Specification schedule requirement.

C9. Individual ordering locations will, upon request, identify which of the above constituent organisation parts they fall within as part of their sub account set ups with the Supplier.

Supplier's Performance Reporting

C10. The Supplier is required to report various Contract Management Information throughout the life of the Agreement to the Authority's Operational Contract Manager. Performance reporting shall be supplied in an electronic format in line with the frequencies specified in the table below.

	Reports	Frequency	Description

A	KPI Summary Report including Lead-time Fulfilment Report	**Monthly** within 5 working days of the month end	Report highlighting lead-times & fulfilment for delivery of Goods including agreed and actual delivery and installation dates
B	Service Performance Report	**Monthly** within 5 working days of the month end	Report highlighting Service attendance timeframes & performance.
C	Proof of Delivery Report	Ad hoc upon request (5 day lead time)	Report showing proof of deliveries requested and copies of delivery documentation.
D	Report showing breakdown of Goods ordered	**Monthly** within 5 working days of the month end	A Management Information Dashboard showing Goods bought over the period, broken down by item and spend and showing predicted lead times against actual delivery times for the Goods.

Key Performance Indicators

C11. Throughout the life of the Contract, the Supplier's performance will be measured and reported against Key Performance Indicators for each month as detailed in the table below.

Table Heading Definitions

(a) KPI – Key Performance Indicator Name

(b) Key Indicators – A brief description of the KPI and what the measurement relates to

(c) Service Level – The level of service which is to be delivered by the Supplier during the life of the Contract. Percentage compliance is measured on an Annual basis against Call Offs.

	(a) KPI	**(b) Key indicators**	**(c) Service Level**
A	% of Delivery Lead Times and Order Fulfilment within agreed lead-times	Within agreed lead-times measured from date of PO transmission to date stated on delivery note.	95% delivered to schedule

	(a) KPI	(b) Key indicators	(c) Service Level
B	Services delivered on time against agreed timescales	Agreed lead-times	98% delivery within agreed date
C	Call Out Attendance	Agreed lead-times	98% within agreed lead times
D	Proof of Delivery	Proof of Delivery (P.O.D) provided within 5 working days of request.	98% provided within 5 working days

Service Improvements Notification

C12. Non- Compliance with the above performance targets may result in one written warning to implement an agreed Service Improvement Plan within 10 Working Days and thereafter for repeated or material ongoing poor performance termination shall be issued (notice period as per Terms and Conditions).

C13. Service improvement plans will be submitted within 10 working days unless otherwise agreed between the parties. The plan will incorporate the Supplier's proposals for improvement over a four week period, at the end of which service levels are to be returned to the agreed levels.

C14. For minor, accepted or agreed non-compliance the Authority may take measures including:

(a) Temporary purchase of specifically affected items from an alternate source until satisfactory improvement has been demonstrated.

(b) Permanent removal of specifically affected items from the Contract (including directly related items).

(c) Enhanced monitoring of Key Performance Indicators and Service Levels and increase in the frequency of requests for information.

(d) Requesting face to face meetings or site visits to propose solution within agreed timescales.

C15. In keeping with the vision of the Contract, both parties will work co-operatively to improve Service Levels to an acceptable standard before reverting to formal improvement measures.

Service Improvement Notices & Plans

C16. Each Service Improvement Notice will require the Supplier to submit a Service Improvement Plan. Each Improvement Plan shall be sequentially numbered from a central register maintained by the Authority.

C17.The Service Improvement Notice and subsequent plan will be applicable to all instances where the nature of the failure or complaint is related to one common service element e.g. if the Supplier fails to adhere to the Framework Agreement or Call Off Contract requirements for compliant order requests to be delivered within the agreed timescales, they may be issued with a Service Improvement Notice by the Authority. Any subsequent failure (subject to the duration of the improvement notice) to submit the same, irrespective of location, type or requestor, will be considered to be within the scope of the original improvement notice.

C18. In the event a further unconnected circumstance occurs which results in the failure to meet the contract requirements a separate Improvement Notice/Plan shall be issued /requested and recorded in the central register under a separate sequential number.

C19. A report on progress against each open Improvement Plan shall be provided at each Contract Review Meeting or as requested.

Contract Management Meetings

C20. The Authority reserves the right to hold regular contract management meetings principally to review progress and operational delivery of the Contract, but also including key performance indicators (KPIs), invoicing, risks and issues.

C21. Other meetings may be held, at the discretion of the Authority or at the request of the Supplier, throughout the life of the contract.

C22. The Supplier will be responsible for associated costs in attending these meetings.

C23. Quarterly and Annual meetings and shall be teleconference calls unless the Authority requires a face to face meeting.

C24. Agendas for meetings will be defined in greater detail throughout the life of the contract but are likely to consist of the following:

Meeting	Content
Mobilisation Meeting	• Introductions • Roles & Responsibilities • Doing Business with the MoJ • Supplier Performance/KPIs • Sustained Supply/Contingency • Ongoing Contract management
Quarterly/ Six Monthly Contract Review Meeting	• Performance in previous quarter • Risks, issues and actions register • Specific service issues (including any escalated issues) • Price Review (where applicable) • Service wide issues • Quality Management • Detailed review against KPIs • Continuous Improvement
Annual Review Meeting	• Annual Service Review • Performance in previous year • Risks, issues and actions register • Specific service issues (including any escalated issues) • Service wide issues • Quality management • Detailed review against KPIs, • Continuous improvement • Service and finance forward look, including any policy update from the Authority

APPENDIX D SPECIAL CONDITIONS PRISONS

[REDACTED DUE TO OPERATIONAL AND COMMERCIAL SENSITIVITY]

SCHEDULE 2 – PRICES AND PAYMENT

1. Charges

1.1 Pricing for equipment, spare parts and services will be in compliance with this contract schedule. All Prices & Rates contained within the Pricing Schedule are exclusive of VAT.

1.2 The Supplier's schedule of rates will form part of the Contract where any services shall be calculated in accordance with these rates.

1A. Goods

[REDACTED DUE TO OPERATIONAL AND COMMERCIAL SENSITIVITY]

1B. Services

[REDACTED DUE TO OPERATIONAL AND COMMERCIAL SENSITIVITY]

1C. Deliveries

[REDACTED DUE TO OPERATIONAL AND COMMERCIAL SENSITIVITY]

2. Milestone Payments

Not used

3. Liquidated Damages

Not used

4. Contract Pricing Duration

5.1 Rates will be firm for the first 12 (twelve) months of the contract after such time the Supplier will be permitted to request annual pricing reviews to coincide with the anniversary of the Contract on each subsequent anniversary.

5. Pricing Review Process

5.1 The Supplier may apply for a price review of rates to coincide with the anniversary of the Contract. The Supplier shall, in the 3 (three) month period prior to the anniversary of the Contract, submit details of the Price Review request and supporting evidence for consideration by the Authority.

5.2 Any increase in the Contract Price (to the relevant Services and/or Goods) shall not exceed the percentage change in the Average Earnings Index in the twelve (12) months preceding the anniversary of the contract (for services), or, for Goods the lesser of:

- the Office of National Statistics' Consumer Prices Index ("**CPI**") agreed product division group in the twelve (12) months preceding the anniversary of the Framework Agreement; or
- indexation in relation to metal markets for raw materials (with overheads and other materials capped at CPI).

5.3 All requests for price increases will be subject to the supplier providing actual documented evidence of an unavoidable increase in costs through the supply chain at component level and unavoidable operational costs. This should include a full breakdown of the component product price and the relevant change request including invoices evidencing the component increase.

5.4 Where an increase is unavoidable the Supplier will be expected to consider re-sourcing product lines, rationalisation or other efficiencies to offset the net impact on the Authority.

5.5 Where there is a change in market forces, technology and product cycle cost reduction and/or CPI & RPI reduction, improved currency conversions, which leads to a decrease in product costs, the Authority will submit a request for price variance for the affected lines. The Authority reserves the right to request a price review where commodity price falls at any time during the life of the Contract.

5.6 Upon non- agreement of any request for price increase, the Authority reserves the right to source products from an alternative route or terminate the Contract.

5.7 Payment Terms

6.7.1 Payment terms are 30 days from the Authority's receipt of Goods following delivery / installation and Supplier's compliant invoice submission to the MoJ Shared Services Centre.

5.8 Invoice Submission

6.8.1 Supplier's invoices shall be submitted to the following address based on the method of payment:

MoJ Shared Services
PO Box 741
Newport
Gwent
NP10 8FZ

Or email electronically to: APinvoices-NMS@gov.sscl.com

5.8.2 All invoices are subject to a three-way matching process prior to payment being made to the Supplier. The Supplier shall ensure that there is no discrepancy between the invoice lines, quantity and price from the original purchase order. Failure to submit a compliant invoice will result in the payment going on hold.

6.8.3 Invoices must be compliant with the following:

(a) Must be received at the correct billing address
(b) Must quote a valid Purchase Order Number (clearly printed on the PO)
(c) Must be to a total agreed sum

(d) Should not be sent to delivery address or with delivery note
(e) Must list product lines broken down by product code
(f) Must give quantity purchased, and individual prices in addition to a line total
(g) Back Order Notification.

6. Payment to Subcontractors

6.1 Where the Supplier enters into a sub-contract with a supplier or contractor for the purpose of performing its obligations under the Contract, it shall ensure that a provision is included in such a sub-contract which requires payment to be made of all sums due by the Supplier to the Sub-Contractor within a specified period not exceeding 30 days from the receipt of a valid invoice.

6.2 Where ad-hoc maintenance Services/ spares are provided, Orders will be placed and payments will be made directly to the Supplier's Sub -Contractor.

7. Credit Notes and Invoice Holds

7.1 Where the Authority has been over invoiced or a price discrepancy has been made by the Supplier a credit note will be required to be raised by the Supplier for the disputed sum to allow payment of the remaining balance. Credit notes will be required to be raised within 4 weeks.

7.2 Payments will be delayed where the Supplier's invoice does not match the original purchase order. All invoices shall match the original purchase order price and format to prevent the invoice from going on hold.

SCHEDULE 3 - CHANGE CONTROL

Changes shall be made in accordance with the process outlined at Clause F4 of the Terms and Conditions and requested using the Change Request Form.

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 E5 (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

SCHEDULE 5 - SUPPLIER AND THIRD PARTY SOFTWARE

Not applicable

SCHEDULE 6 – INFORMATION ASSURANCE & SECURITY

1. GENERAL

1.1 This Schedule 6 sets out the obligations of the Parties in relation to information assurance and security, including those which the Supplier must comply with in delivering the Services under the Contract.

1.2 The Parties acknowledge that the purpose of the ISMS and Security Plan is to ensure a robust organisational approach to information assurance and security under which the specific requirements of the Contract will be met.

1.3 The Parties shall each appoint and/or identify a board level individual or equivalent who has overall responsibility for information assurance and security, including personnel security and information risk. The individual appointed by the Supplier, who is the Chief Security Officer, Chief Information Officer, Chief Technical Officer or equivalent and is responsible for compliance with the ISMS, is identified as Key Personnel) and the provisions of clause B11 apply in relation to that person.

1.4 The Supplier shall act in accordance with Good Industry Practice in the day to day operation of any system which is used for the storage of Information Assets and/or the storage, processing or management of Authority Data and/or that could directly or indirectly affect Information Assets and/or Authority Data.

1.5 The Supplier shall ensure that an information security policy is in place in respect of the operation of its organisation and systems, which shall reflect relevant control objectives for the Supplier System, including those specified in the ISO27002 control set or equivalent, unless otherwise agreed by the Authority. The Supplier shall, upon request, provide a copy of this policy to the Authority as soon as reasonably practicable. The Supplier shall maintain and keep such policy updated and provide clear evidence of this as part of its Security Plan.

1.6 The Supplier acknowledges that a compromise of Information Assets and/or Authority Data represents an unacceptable risk to the Authority requiring immediate communication and co-operation between the Parties. The Supplier shall provide clear evidence of regular communication with the Authority in relation to information risk as part of its Security Plan.

2. INFORMATION SECURITY MANAGEMENT SYSTEM

2.1 The Supplier shall, within 30 Working Days of the Commencement Date, submit to the Authority a proposed ISMS which:

2.1.1 has been tested; and

2.1.2 complies with the requirements of paragraphs 2.2 and 2.3.

2.2 The Supplier shall at all times ensure that the level of security, include cyber security, provided by the ISMS is sufficient to protect the confidentiality, integrity and availability of Information Assets and Authority Data used in the provision of the Services and to provide robust risk management.

2.3 The Supplier shall implement, operate and maintain an ISMS which shall:

2.3.1 protect all aspects of and processes of Information Assets and Authority Data, including where these are held on the ICT Environment (to the extent that this is under the control of the Supplier);

2.3.2 be aligned to and compliant with the relevant standards in ISO/IEC 27001: 2013 or equivalent and the Certification Requirements in accordance with paragraph 5 unless otherwise Approved;

2.3.3 provide a level of security which ensures that the ISMS and the Supplier System:

2.3.3.1 meet the requirements in the Contract;

2.3.3.2 are in accordance with applicable Law;

2.3.3.3 demonstrate Good Industry Practice, including the Government's 10 Steps to Cyber Security, currently available at:

https://www.ncsc.gov.uk/guidance/10-steps-cyber-security;

2.3.3.4 comply with the Security Policy Framework and any other relevant Government security standards;

2.3.3.5 comply with the Baseline Security Requirements;

2.3.3.6 comply with the Authority's policies, including, where applicable, PSI 24/2014;

2.3.4 address any issues of incompatibility with the Supplier's organisational security policies;

2.3.5 address any specific security threats of immediate relevance to Information Assets and/or Authority Data;

2.3.6 document:

2.3.6.1 the security incident management processes, including reporting, recording and management of information risk incidents, including those relating to the ICT Environment (to the extent that this is within the control of the Supplier) and the loss of protected Personal Data, and the procedures for reducing and raising awareness of information risk;

2.3.6.2 incident response plans, including security incident response companies; and

2.3.6.3 the vulnerability management policy, including processes for identification of system vulnerabilities and assessment of the potential effect on the Services of any new threat, vulnerability or exploitation technique of which the Supplier becomes aware, prioritisation of security patches, testing and application of application of security patches and the reporting and audit mechanism detailing the efficacy of the patching policy;

2.3.7 include procedures for the secure destruction of Information Assets and Authority Data and any hardware or devices on which such information or data is stored; and

2.3.8 be certified by (or by a person with the direct delegated authority of) the Supplier's representative appointed and/or identified in accordance with paragraph 1.3.

2.4 If the Supplier becomes aware of any inconsistency in the provisions of the standards, guidance and policies notified to the Supplier from time to time, the Supplier shall immediately notify the Authority of such inconsistency and the Authority shall, as soon as practicable, notify the Supplier of the provision that takes precedence.

2.5 The Supplier shall, upon request from the Authority or any accreditor appointed by the Authority, provide sufficient design documentation detailing the security architecture of its ISMS to support the Authority's and/or accreditor's assurance that it is appropriate, secure and complies with the Authority's requirements.

2.6 The Authority shall review the proposed ISMS submitted pursuant to paragraph 2.1 and shall, within 10 Working Days of its receipt notify the Supplier as to whether it has been approved.

2.7 If the ISMS is Approved, it shall be adopted by the Supplier immediately and thereafter operated and maintained throughout the Term in accordance with this Schedule 6.

2.8 If the ISMS is not Approved, the Supplier shall amend it within 10 Working Days of a notice of non-approval from the Authority and re-submit it to the Authority for approval. The Authority shall, within a further 10 Working Days notify the Supplier whether the amended ISMS has been approved. The Parties shall use reasonable endeavours to ensure that the approval process takes as little time as possible and in any event no longer than 30 Working Days from the date of its first submission to the Authority. If the Authority does not approve the ISMS following its resubmission, the matter shall be resolved in accordance with clause I1 (Dispute Resolution).

2.9 Approval of the ISMS or any change to it shall not relieve the Supplier of its obligations under this Schedule 6.

2.10 The Supplier shall provide to the Authority, upon request, any or all ISMS documents.

3. SECURITY PLAN

3.1 The Supplier shall, within 30 Working Days of the Commencement Date, submit to the Authority for approval a Security Plan which complies with paragraph 3.2.

3.2 The Supplier shall effectively implement the Security Plan which shall:

3.2.1 comply with the Baseline Security Requirements;

3.2.2 identify the organisational roles for those responsible for ensuring the Supplier's compliance with this Schedule 6;

3.2.3 detail the process for managing security risks from those with access to Information Assets and/or Authority Data, including where these are held in the ICT Environment;

3.2.4 set out the security measures and procedures to be implemented by the Supplier, which are sufficient to ensure compliance with the provisions of this Schedule 6;

3.2.5 set out plans for transition from the information security arrangements in place at the Commencement Date to those incorporated in the ISMS;

3.2.6 set out the scope of the Authority System that is under the control of the Supplier;

3.2.7 be structured in accordance with ISO/IEC 27001: 2013 or equivalent unless otherwise Approved;

3.2.8 be written in plain language which is readily comprehensible to all Staff and to Authority personnel engaged in the Services and reference only those documents which are in the possession of the Parties or whose location is otherwise specified in this Schedule 6; and

3.2.9 comply with the Security Policy Framework and any other relevant Government security standards.

3.3 The Authority shall review the Security Plan submitted pursuant to paragraph 3.1 and notify the Supplier, within 10 Working Days of receipt, whether it has been approved.

3.4 If the Security Plan is Approved, it shall be adopted by the Supplier immediately and thereafter operated and maintained throughout the Term in accordance with this Schedule 6.

3.5 If the Security Plan is not Approved, the Supplier shall amend it within 10 Working Days of a notice of non-approval from the Authority and re-submit it to the Authority for approval. The Authority shall notify the Supplier within a further 10 Working Days whether it has been approved.

3.6 The Parties shall use reasonable endeavours to ensure that the approval process takes as little time as possible and in any event no longer than 30 Working Days from the date of its first submission to the Authority. If the Authority does not approve the Security Plan following its resubmission, the matter shall be resolved in accordance with clause I1 (Dispute Resolution).

3.7 Approval by the Authority of the Security Plan pursuant to paragraph 3.3 or of any change to the Security Plan shall not relieve the Supplier of its obligations under this Schedule 6.

4. REVISION OF THE ISMS AND SECURITY PLAN

4.1 The ISMS and Security Plan shall be reviewed in full and tested by the Supplier at least annually throughout the Term (or more often where there is a significant change to the Supplier System or associated processes or where an actual or potential Breach of Security or weakness is identified) to consider and take account of:

4.1.1 any issues in implementing the Security Policy Framework and/or managing information risk;

4.1.2 emerging changes in Good Industry Practice;

4.1.3 any proposed or actual change to the ICT Environment and/or associated processes;

4.1.4 any new perceived, potential or actual security risks or vulnerabilities;

4.1.5 any ISO27001: 2013 audit report or equivalent produced regarding the Certification Requirements which indicates concerns; and

4.1.6 any reasonable change in security requirements requested by the Authority.

4.2 The Supplier shall give the Authority the results of such reviews as soon as reasonably practicable after their completion, which shall include without limitation:

4.2.1 suggested improvements to the effectiveness of the ISMS, including controls;

4.2.2 updates to risk assessments; and

4.2.3 proposed modifications to respond to events that may affect the ISMS, including the security incident management processes, incident response plans and general procedures and controls that affect information security.

4.3 Following the review in accordance with paragraphs 4.1 and 4.2 or at the Authority's request, the Supplier shall give the Authority at no additional cost a draft updated ISMS and/or

Security Plan which includes any changes the Supplier proposes to make to the ISMS or Security Plan. The updated ISMS and/or Security Plan shall, unless otherwise agreed by the Authority, be subject to clause F4 (Change) and shall not be implemented until Approved.

4.4 If the Authority requires any updated ISMS and/or Security Plan to be implemented within shorter timescales than those set out in clause F4, the Parties shall thereafter follow clause F4 for the purposes of formalising and documenting the relevant change for the purposes of the Contract.

5. CERTIFICATION REQUIREMENTS

5.1 The Supplier shall ensure that any systems, including the ICT Environment, on which Information Assets and Authority Data are stored and/or processed are certified as compliant with:

5.1.1 ISO/IEC 27001:2013 or equivalent by a UKAS approved certification body or are included within the scope of an existing certification of compliance with ISO/IEC 27001:2013 or equivalent unless otherwise Approved; and

5.1.2 the Government's Cyber Essentials Scheme at the BASIC level unless otherwise agreed with the Authority

and shall provide the Authority with evidence:

5.1.3 of certification before the Supplier accessed the ICT Environment and receives, stores, processes or manages any Authority Data; and

5.1.4 that such certification remains valid and is kept up to date while the Supplier (as applicable) continues to access the ICT Environment and receives, stores, processes or manages any Authority Data during the Term.

5.2 The Supplier shall ensure that it:

5.2.1 carries out any secure destruction of Information Assets and/or Authority Data at Supplier sites which are included within the scope of an existing certificate of compliance with ISO/IEC 27001:2013 or equivalent unless otherwise Approved; and

5.2.2 is certified as compliant with the CESG Assured Service (CAS) Service Requirement Sanitisation Standard or equivalent unless otherwise Approved

and the Supplier shall provide the Authority with evidence of its compliance with the requirements set out in this paragraph 5.2 before the Supplier may carry out the secure destruction of any Information Assets and/or Authority Data.

5.3 The Supplier shall notify the Authority as soon as reasonably practicable and, in any event within 2 Working Days, if the Supplier ceases to be compliant with the certification requirements in paragraph 5.1 and, on request from the Authority, shall:

5.3.1 immediately cease access to and use of Information Assets and/or Authority Data; and

5.3.2 promptly return, destroy and/or erase any Authority Data in accordance with the Baseline Security Requirements

and failure to comply with this obligation is a material Default.

6. SECURITY TESTING

6.1 The Supplier shall, at its own cost, carry out relevant Security Tests from the Commencement Date and throughout the Term, which shall include:

6.1.1 a monthly vulnerability scan and assessment of the Supplier System and any other system under the control of the Supplier on which Information Assets and/or Authority Data are held;

6.1.2 an annual IT Health Check by an independent qualified company of the Supplier System and any other system under the control of the Supplier on which Information Assets and/or Authority Data are held and any additional IT Health Checks required by the Authority and/or any accreditor;

6.1.3 an assessment as soon as reasonably practicable following receipt by the Supplier of a critical vulnerability alert from a provider of any software or other component of the Supplier System and/or any other system under the control of the Supplier on which Information Assets and/or Authority Data are held; an

6.1.4 such other tests as are required:

6.1.4.1 by any Vulnerability Correction Plans;

6.1.4.2 by ISO/IEC 27001:2013 certification requirements or equivalent Approved;

6.1.4.3 after any significant architectural changes to the ICT Environment;

6.1.4.4 after a change to the ISMS (including security incident management processes and incident response plans) or the Security Plan; and

6.1.4.5 following a Breach of Security.

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

6.2.1 agree with the Authority the aim and scope of the IT Health Check;

6.2.2 promptly, following receipt of each IT Health Check report, give the Authority a copy of the IT Health Check report;

6.2.3 if the IT Health Check report identifies any vulnerabilities:

6.2.3.1 prepare a Vulnerability Correction Plan for Approval which sets out in respect of each such vulnerability:

6.2.3.1.1 how the vulnerability will be remedied;

6.2.3.1.2 the date by which the vulnerability will be remedied;

6.2.3.1.3 the tests which the Supplier shall perform or procure to be performed (which may, at the Authority's discretion, include a further IT Health Check) to confirm that the vulnerability has been remedied;

6.2.3.2 comply with the Vulnerability Correction Plan; and

6.2.3.3 conduct such further Security Tests as are required by the Vulnerability Correction Plan.

6.3 Security Tests shall be designed and implemented by the Supplier to minimise any adverse effect on the Services and the date, timing, content and conduct of Security Tests shall be agreed in advance with the Authority.

6.4 The Authority may send a representative to witness the conduct of the Security Tests. The Supplier shall provide the Authority with the results of Security Tests (in a form to be Approved) as soon as practicable and in any event within 5 Working Days after completion of each Security Test.

6.5 Without prejudice to any other right of audit or access granted to the Authority pursuant to the Contract, the Authority and/or its authorised representatives, including any accreditor, may at any time to carry out Security Tests (including penetration tests) as it may deem necessary as part of any accreditation process and/or to verify the Supplier's compliance with the ISMS and the Security Plan:

6.5.1 upon giving reasonable notice to the Supplier where reasonably practicable to do so; and

6.5.2 without giving notice to the Supplier where, in the Authority's view, the provision of such notice may undermine the Security Tests to be carried out

and, where applicable, the Authority shall be granted access to the Supplier's premises for the purpose of undertaking the relevant Security Tests.

6.6 If the Authority carries out Security Tests in accordance with paragraphs 6.5.1 or 6.5.2, the Authority shall (unless there is any reason to withhold such information) notify the Supplier of the results of the Security Tests as soon as possible and in any event within 5 Working Days after completion of each Security Test.

6.7 If any Security Test carried out pursuant to paragraphs 6.1 or 6.4 reveals any:

6.7.1 vulnerabilities during any accreditation process, the Supplier shall track and resolve them effectively; and

6.7.2 actual or potential Breach of Security or weaknesses (including un-patched vulnerabilities, poor configuration and/or incorrect system management), the Supplier shall promptly notify the Authority of any proposed changes to the ICT Environment (to the extent that this is under the control of the Supplier) and/or to the ISMS and/or to the Security Plan (and the implementation thereof) which the Supplier intends to make in order to correct such failure or weakness. Subject to Approval and paragraphs 4.3 and 4.4, the Supplier shall implement such changes to the ICT Environment (to the extent that this is under the control of the Supplier) and/or the ISMS and/or the Security Plan and repeat the relevant Security Tests in accordance with an Approved timetable or, otherwise, as soon as reasonably practicable.

6.8 If the Authority unreasonably withholds its approval to the implementation of any changes to the ICT Environment and/or to the ISMS and/or to the Security Plan proposed by the Supplier in accordance with paragraph 6.7, the Supplier is not in breach of the Contract to the extent that it can be shown that such breach:

6.8.1 has arisen as a direct result of the Authority unreasonably withholding Approval to the implementation of such proposed changes; and

6.8.2 would have been avoided had the Authority Approved the implementation of such proposed changes.

6.9 If a change to the ISMS or Security Plan is to address any non-compliance with ISO/IEC 27001:2013 requirements or equivalent, the Baseline Security Requirements or any obligations in the Contract, the Supplier shall implement such change at its own cost and expense.

6.10 If any repeat Security Test carried out pursuant to paragraph 6.7 reveals an actual or potential breach of security or weakness exploiting the same root cause failure, such circumstance shall constitute a material Default.

6.11 On each anniversary of the Commencement Date, the Supplier shall provide to the Authority a letter from the individual appointed or identified in accordance with paragraph 1.3 confirming that having made due and careful enquiry:

6.11.1 the Supplier has in the previous year carried out all Security Tests in accordance with this Schedule 6 and has complied with all procedures in relation to security matters required under the Contract; and

6.11.2 the Supplier is confident that its security and risk mitigation procedures in relation to Information Assets and Authority Data remain effective.

7. SECURITY AUDITS AND COMPLIANCE

7.1 The Authority and its authorised representatives may carry out security audits as it reasonably considers necessary in order to ensure that the ISMS is compliant with the principles and practices of ISO 27001: 2013 or equivalent (unless otherwise Approved), the requirements of this Schedule 6 and the Baseline Security Requirements.

7.2 If ISO/IEC 27001: 2013 certification or equivalent is provided, the ISMS shall be audited independently in accordance with ISO/IEC 27001: 2013 or equivalent. The Authority and its authorised representatives shall, where applicable, be granted access to the Supplier Sites and Sub-contractor premises for this purpose.

7.3 If, on the basis of evidence resulting from such audits, it is the Authority's reasonable opinion that ISMS is not compliant with any applicable principles and practices of ISO/IEC 27001: 2013 or equivalent, the requirements of this Schedule 6 and/or the Baseline Security Requirements is not being achieved by the Supplier, the Authority shall notify the Supplier of this and provide a reasonable period of time (having regard to the extent and criticality of any non-compliance and any other relevant circumstances) for the Supplier to implement any necessary remedy. If the Supplier does not ensure that the ISMS is compliant within this period of time, the Authority may obtain an independent audit of the ISMS to assess compliance (in whole or in part).

7.4 If, as a result of any such independent audit as described in paragraph 7.3 the Supplier is found to be non-compliant with any applicable principles and practices of ISO/IEC 27001:2013 or equivalent, the requirements of this Schedule 6 and/or the Baseline Security Requirements the Supplier shall, at its own cost, undertake those actions that are required in order to ensure that the ISMS is complaint and shall reimburse the Authority in full in respect of the costs obtaining such an audit.

8. SECURITY RISKS AND BREACHES

8.1 The Supplier shall use its reasonable endeavours to prevent any Breach of Security for any reason, including as a result of malicious, accidental or inadvertent behaviour.

8.2 If either Party becomes aware of a Breach of Security or an attempted Breach of Security it shall act in accordance with the agreed security incident management processes and incident response plans as set out in the ISMS.

8.3 Without prejudice to the security incident management processes and incident response plans set out in the ISMS and any requirements to report incidents in accordance with PSI 24/2014, upon becoming aware of any Breach of Security or attempted Breach of Security, the Supplier shall:

8.3.1 immediately notify the Authority and take all reasonable steps (which shall include any action or changes reasonably required by the Authority) that are necessary to:

8.3.1.1 minimise the extent of actual or potential harm caused by any Breach of Security;

8.3.1.2 remedy any Breach of Security to the extent that is possible and protect the integrity of the ICT Environment (to the extent that this is within its control) and ISMS against any such Breach of Security or attempted Breach of Security;

8.3.1.3 mitigate against a Breach of Security or attempted Breach of Security; and

8.3.1.4 prevent a further Breach of Security or attempted Breach of Security in the future resulting from the same root cause failure;

8.3.2 provide to the Authority and/or the Computer Emergency Response Team for UK Government ("**GovCertUK**") or equivalent any data that is requested relating to the Breach of Security or attempted Breach of Security within 2 Working Days of such request; and

8.3.3 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 (using the reporting mechanism defined by the ISMS) of the Breach of Security or attempted Breach of Security, including a root cause analysis if required by the Authority

and the Supplier recognises that the Authority may report significant actual or potential losses of Personal Data to the Information Commissioner or equivalent and to the Cabinet Office.

8.4 If any action is taken by the Supplier in response to a Breach of Security or attempted Breach of Security which occurred as a result of non-compliance of the ISMS with any ISO/IEC 27001: 2013 requirements or equivalent (as applicable), the Baseline Security Requirements and/or the requirements of this Schedule 6, any such action and change to the ISMS and/or Security Plan as a result shall be implemented at the Supplier's cost.

IT Environment

8.5 The Supplier shall ensure that the Supplier System:

8.5.1 functions in accordance with Good Industry Practice for protecting external connections to the internet;

8.5.2 functions in accordance with Good Industry Practice for protection from malicious code;

8.5.3 provides controls to securely manage (store and propagate) all cryptographic keys to prevent malicious entities and services gaining access to them, in line with the Authority's Cryptographic Policy as made available to the Supplier from time to time;

8.5.4 is patched (and all its components are patched) in line with Good Industry Practice, any Authority patching policy currently in effect and notified to the Supplier and any Supplier patch policy that is agreed with the Authority; and

8.5.5 uses the latest versions of anti-virus definitions, firmware and software available from industry accepted anti-virus software vendors.

8.6 Notwithstanding paragraph 8.5, if a Breach of Security is detected in the ICT Environment, the Parties shall co-operate to reduce the effect of the Breach of Security and, if the Breach of Security causes loss of operational efficiency or loss or corruption of Information Assets and/or Authority Data, assist each other to mitigate any losses and to recover and restore such Information Assets and Authority Data.

8.7 All costs arising out of the actions taken by the Parties in compliance with paragraphs 8.2, 8.3 and 8.6 shall be borne by:

8.7.1 the Supplier if the Breach of Security originates from the defeat of the Supplier's security controls or Information Assets and/or Authority Data is lost or corrupted whilst under the control of the Supplier or its Sub-contractor; or

8.7.2 the Authority if the Breach of Security originates from the defeat of the Authority's security controls or Information Assets and/or Authority Data is lost or corrupted whilst under the control of the Authority

and each Party shall bear its own costs in all other cases.

9. VULNERABILITIES AND CORRECTIVE ACTION

9.1 The Parties acknowledge that from time to time vulnerabilities in the ICT Environment and ISMS will be discovered which, unless mitigated, will present an unacceptable risk to Information Assets and/or Authority Data.

9.2 The severity of any vulnerabilities shall be categorised by the Supplier as '*Critical*', '*Important*' and '*Other*' according to the agreed method in the ISMS and using any appropriate vulnerability scoring systems.

9.3 The Supplier shall procure the application of security patches to vulnerabilities categorised as '*Critical*' within 7 days of public release, vulnerabilities categorised as '*Important*' within 30 days of public release and vulnerabilities categorised as '*Other*' within 60 days of public release, except where:

9.3.1 the Supplier can demonstrate that a vulnerability is not exploitable within the context of the Services being provided, including where it resides in a software component which is not being used, provided that, where those vulnerabilities become exploitable, they are remedied by the Supplier within the timescales in paragraph 9.3;

9.3.2 the application of a security patch in respect of a vulnerability categorised as '*Critical*' or '*Important*' adversely affects the Supplier's ability to deliver the Services, in which case the Supplier shall be granted an extension to the timescales in paragraph 9.3 of 5 days, provided that the Supplier continues to follow any security patch test plan agreed with the Authority; or

9.3.3 the Authority agrees a different timescale after consultation with the Supplier in accordance with the processes defined in the ISMS.

9.4 The ISMS and the Security Plan shall include provision for the Supplier to upgrade software throughout the Term within 6 months of the release of the latest version unless:

9.4.1 upgrading such software reduces the level of mitigation for known threats, vulnerabilities or exploitation techniques, provided always that such software is upgraded by the Supplier within 12 months of release of the latest version; or

9.4.2 otherwise Approved.

9.5 The Supplier shall:

9.5.1 implement a mechanism for receiving, analysing and acting upon threat information provided by GovCertUK, or any other competent Central Government Body;

9.5.2 ensure that the ICT Environment (to the extent that this is within the control of the Supplier) is monitored to facilitate the detection of anomalous behaviour that would be indicative of system compromise;

9.5.3 ensure that it is knowledgeable about the latest trends in threat, vulnerability and exploitation that are relevant to the ICT Environment (to the extent that this is within the control of the Supplier) by actively monitoring the threat landscape during the Term;

9.5.4 pro-actively scan the ICT Environment (to the extent that this is within the control of the Supplier) for vulnerable components and address discovered vulnerabilities through the processes described in the ISMS;

9.5.5 from the Commencement Date and within 5 Working Days of the end of each subsequent month during the Term provide a report to the Authority detailing both patched and outstanding vulnerabilities in the ICT Environment (to the extent that this is within the control of the Supplier) and any elapsed time between the public release date of patches and either the time of application or, for outstanding vulnerabilities, the time of issue of such report;

9.5.6 propose interim mitigation measures in respect of any vulnerabilities in the ICT Environment (to the extent this is within the control of the Supplier) known to be exploitable where a security patch is not immediately available;

9.5.7 remove or disable any extraneous interfaces, services or capabilities that are no longer needed for the provision of the Services (in order to reduce the attack surface of the ICT Environment to the extent this is within the control of the Supplier); and

9.5.8 inform the Authority when it becomes aware of any new threat, vulnerability or exploitation technique that has the potential to affect the security of the IT Environment (to the extent this is within the control of the Supplier) and provide initial indications of possible mitigations

9.6 If the Supplier is unlikely to be able to mitigate any vulnerability within the timescales in paragraph 9.3, the Supplier shall notify the Authority immediately.

9.7 Any failure by the Supplier to comply with paragraph 9.3 shall constitute a material Default.

10. SUB-CONTRACTS

10.1 The Supplier shall ensure that all Sub-Contracts with Sub-Contractors who have access to Information Assets and/or Authority Data contain equivalent provisions in relation to information assurance and security that are no less onerous than those imposed on the Supplier under the Contract.

ANNEXE 1 – BASELINE SECURITY REQUIREMENTS

1 Security Classifications and Controls

1.1 The Supplier shall, unless otherwise Approved in accordance with paragraph 6.2 of this Annexe 1, only have access to and handle Information Assets and Authority Data that are classified under the Government Security Classifications Scheme as OFFICIAL.

1.2 There may be a specific requirement for the Supplier in some instances on a limited 'need to know basis' to have access to and handle Information Assets and Authority Data that are classified as 'OFFICIAL-SENSITIVE.'

1.3 The Supplier shall apply the security controls required for OFFICIAL information and OFFICIAL-SENSITIVE information as described in Cabinet Office guidance, currently at:

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/251480/Government-Security-Classifications-April-2014.pdf.

1.4 The Supplier shall be able to demonstrate to the Authority and any accreditor that it has taken into account the "Technical Controls Summary" for OFFICIAL (in the above guidance) in designing and implementing the security controls in the Supplier System, which shall be subject to assurance and accreditation to Government standards.

1.5 Additional controls may be required by the Authority and any accreditor where there are aspects of data aggregation.

2 End User Devices

2.1 Authority Data shall, wherever possible, be held and accessed on paper or in the ICT Environment on secure premises and not on removable media (including laptops, removable discs, CD-ROMs, USB memory sticks, PDAs and media card formats) without Approval. If Approval is sought to hold and access data by other means, the Supplier shall consider the second-best option and third best option below and record the reasons why a particular approach should be adopted when seeking Approval:

2.1.1 second best option means: secure remote access so that data can be viewed or amended over the internet without being permanently stored on the remote device, using products meeting the FIPS 140-2 standard or equivalent, unless Approved;

2.1.2 third best option means: secure transfer of Authority Data to a remote device at a secure site on which it will be permanently stored, in which case the Authority Data and any links to it shall be protected at least to the FIPS 140-2 standard or equivalent, unless otherwise Approved, and noting that protectively marked Authority Data must not be stored on privately owned devices unless they are protected in this way.

2.2 The right to transfer Authority Data to a remote device should be carefully considered and strictly limited to ensure that it is only provided where absolutely necessary and shall be subject to monitoring by the Supplier and Authority.

2.3 Unless otherwise Approved, when Authority Data resides on a mobile, removable or physically uncontrolled device, it shall be:

2.3.1 the minimum amount that is necessary to achieve the intended purpose and should be anonymised if possible;

2.3.2 stored in an encrypted form meeting the FIPS 140-2 standard or equivalent and using a product or system component which has been formally assured through a recognised certification process of CESG to at least Foundation Grade, for example,

under the CESG Commercial Product Assurance scheme ("**CPA**") or equivalent, unless otherwise Approved;

2.3.3 protected by an authentication mechanism, such as a password; and

2.3.4 have up to date software patches, anti-virus software and other applicable security controls to meet the requirements of this Schedule 6.

2.4 Devices used to access or manage Authority Data shall be under the management authority of the Supplier and have a minimum set of security policy configurations enforced. Unless otherwise Approved, all Supplier devices shall satisfy the security requirements set out in the CESG End User Devices Platform Security Guidance ("**CESG Guidance**") (https://www.gov.uk/government/collections/end-user-devices-security-guidance--2) or equivalent.

2.5 Where the CESG Guidance highlights shortcomings in a particular platform the Supplier may wish to use, then these should be discussed with the Authority and a joint decision shall be taken on whether the residual risks are acceptable. If the Supplier wishes to deviate from the CESG Guidance, this should be agreed in writing with the Authority on a case by case basis.

3 Data Storage, Processing, Management, Transfer and Destruction

3.1 The Parties recognise the need for Authority Data to be safeguarded and for compliance with the Data Protection Legislation. To that end, the Supplier shall inform the Authority the location within the United Kingdom where Authority Data is stored, processed and managed. The import and export of Authority Data from the Supplier System must be strictly controlled and recorded.

3.2 The Supplier shall inform the Authority of any changes to the location within the United Kingdom where Authority Data is stored, processed and managed and shall not transmit, store, process or manage Authority Data outside of the United Kingdom without Approval which shall not be unreasonably withheld or delayed provided that the transmission, storage, processing and management of Authority Data offshore is within:

3.2.1 the European Economic Area ("**EEA**"); or

3.2.2 another country or territory outside the EEA if that country or territory ensures an adequate level of protection by reason of its domestic law or of the international commitments it has entered into which have been defined as adequate by the European Commission.

3.3 The Supplier System shall support the requirement of the Authority to comply with Government policy and Cabinet Office guidance on Offshoring, currently set out at:

https://ogsirooffshoring.zendesk.com/hc/en-us/articles/203107991-HMG-sOffshoring-Policy

by assessing, as required, any additional security risks associated with the storage, processing and/or transmission of any data and/or information offshore, including by an offshore Supplier (which may include the use of 'landed resources'), taking account of European Union requirements to confirm the 'adequacy' of protection of Personal Data in the countries where storage, processing and/or transmission occurs. No element of the Supplier System may be off-shored without Approval.

3.4 The Supplier shall ensure that the Supplier System provides internal processing controls between security domains to prevent the unauthorised high domain exporting of Authority Data to the low domain if there is a requirement to pass data between different security domains.

3.5 The Supplier shall ensure that any electronic transfer of Authority Data:

3.5.1 protects the confidentiality of the Authority during transfer through encryption suitable for the impact level of the data;

3.5.2 maintains the integrity of the Authority Data during both transfer and loading into the receiving system through suitable technical controls for the impact level of the data; and

3.5.3 prevents the repudiation of receipt through accounting and auditing.

3.6 The Supplier shall:

3.6.1 protect Authority Data, including Personal Data, whose release or loss could cause harm or distress to individuals and ensure that this is handled as if it were confidential while it is stored and/or processed;

3.6.2 ensure that OFFICIAL-SENSITIVE information, including Personal Data is encrypted in transit and when at rest when stored away from the Supplier's controlled environment;

3.6.3 on demand, provide the Authority with all Authority Data in an agreed open format;

3.6.4 have documented processes to guarantee availability of Authority Data if it stops trading;

3.6.5 securely destroy all media that has held Authority Data at the end of life of that media in accordance with any requirements in the Contract and, in the absence of any such requirements, in accordance with Good Industry Practice;

3.6.6 securely erase any or all Authority Data held by the Supplier when requested to do so by the Authority;

3.6.7 ensure that all material used for storage of Confidential Information is subject to controlled disposal and the Supplier shall:

3.6.7.1 destroy paper records containing Personal Data by incineration, pulping or shredding so that reconstruction is unlikely; and

3.6.7.2 dispose of electronic media that was used for the processing or storage of Personal Data through secure destruction, overwriting, erasure or degaussing for re-use.

4 Networking

4.1 Any Authority Data transmitted over any public network (including the Internet, mobile networks or un-protected enterprise network) or to a mobile device shall be encrypted using a product or system component which has been formally assured through a certification process recognised by CESG, to at least Foundation Grade, for example, under CPA or through the use of Public Sector Network ("**PSN**") compliant encrypted networking services or equivalent unless none are available in which case the Supplier shall agree the solution with the Authority.

4.2 The Authority requires that the configuration and use of all networking equipment in relation to the provision of the Services, including equipment that is located in secure physical locations, is at least compliant with Good Industry Practice.

4.3 The Supplier shall ensure that the ICT Environment (to the extent this is within the control of the Supplier) contains controls to maintain separation between the PSN and internet connections if used.

5 Security Architectures

5.1 When designing and configuring the ICT Environment (to the extent that this is within the control of the Supplier) the Supplier shall follow Good Industry Practice and seek guidance from recognised security professionals with the appropriate skills and/or those with a CESG Certified Professional certification

(http://www.cesg.gov.uk/awarenesstraining/IA-certification/Pages/index.aspx)

or equivalent for all bespoke or complex components.

5.2 The Supplier shall provide to the Authority and any accreditor sufficient design documentation detailing the security architecture of the ICT Environment and data transfer mechanism to support the Authority's and any accreditor's assurance that this is appropriate, secure and compliant with the Authority's requirements.

5.3 The Supplier shall apply the '*principle of least privilege*' (the practice of limiting systems, processes and user access to the minimum possible level) to the design and configuration of the ICT Environment used for the storage, processing and management of Authority Data. Users should only be granted the minimum necessary permissions to access Information Assets and Authority Data and must be automatically logged out of the Supplier System if an account or session is inactive for more than 15 minutes.

6 Digital Continuity

The Supplier shall ensure that each Information Asset is held in an appropriate format that is capable of being updated from time to time to enable the Information Asset to be retrieved, accessed, used and transferred to the Authority, including in accordance with any information handling procedures set out in PSI 24/2014.

7 Personnel Vetting and Security

7.1 All Staff shall be subject to pre-employment checks that include, as a minimum, their employment history for at least the last 3 years, identity, unspent criminal convictions and right to work (including nationality and immigration status) and shall be vetted in accordance with:

7.1.1 the BPSS or BS7858 or equivalent; and

7.1.2 PSI 07/2014 based on their level of access to Information Assets and/or Authority Data.

7.2 If the Authority agrees that it is necessary for any Staff to have logical or physical access to Information Assets and/or Authority Data classified at a higher level than OFFICIAL (such as that requiring '*SC*' clearance), the Supplier shall obtain the specific government clearances that are required for access to such Information Assets and/or Authority Data.

7.3 The Supplier shall prevent Staff who are unable to obtain the required security clearances from accessing Information Assets and/or Authority Data and/or the ICT Environment used to store, process and/or manage such Information Assets or Authority Data.

7.4 The Supplier shall procure that all Staff comply with the Security Policy Framework and principles, obligations and policy priorities stated therein, including requirements to manage and report all security risks in relation to the provision of the Services.

7.5 The Supplier shall ensure that Staff who can access Information Assets and/or Authority Data and/or the ICT Environment are aware of their responsibilities when handling such information and data and undergo regular training on secure information management principles. Unless otherwise Approved, this training must be undertaken annually.

7.6 If the Supplier grants Staff access to Information Assets and/or Authority Data, those individuals shall be granted only such levels of access and permissions that are necessary for them to carry out their duties. Once Staff no longer require such levels of access or permissions or leave the organisation, their access rights shall be changed or revoked (as applicable) within one Working Day.

8 Identity, Authentication and Access Control

8.1 The Supplier shall operate a robust role-based access control regime, including network controls, to ensure all users and administrators of and those maintaining the ICT Environment are uniquely identified and authenticated when accessing or administering the ICT Environment to prevent unauthorised users from gaining access to Information Assets and/or Authority Data. Applying the '*principle of least privilege'*, users and administrators and those responsible for maintenance shall be allowed access only to those parts of the ICT Environment they require. The Supplier shall retain an audit record of accesses and users and disclose this to the Authority upon request.

8.2 The Supplier shall ensure that Staff who use the Authority System actively confirm annually their acceptance of the Authority's acceptable use policy.

9 Physical Media

9.1 The Supplier shall ensure that all:

9.1.1 OFFICIAL information is afforded physical protection from internal, external and environmental threats commensurate with the value to the Authority of that information;

9.1.2 physical components of the Supplier System are kept in secure accommodation which conforms to the Security Policy Framework and CESG standards and guidance or equivalent;

9.1.3 physical media holding OFFICIAL information is handled in accordance with the Security Policy Framework and CESG standards and guidance or equivalent; and

9.1.4 Information Assets and Authority Data held on paper are:

9.1.4.1 kept secure at all times, locked away when not in use on the premises on which they are held and secured and are segregated if the Supplier is co-locating with the Authority; and

9.1.4.2 only transferred by an approved secure form of transfer with confirmation of receipt obtained.

10 Audit and Monitoring

10.1 The Supplier shall implement effective monitoring of its information assurance and security obligations in accordance with Government standards and where appropriate, in accordance with CESG Good Practice Guide 13 – Protective Monitoring or equivalent.

10.2 The Supplier shall collect audit records which relate to security events in the ICT Environment (where this is within the control of the Supplier), including those that would support the analysis of potential and actual compromises. In order to facilitate effective monitoring and forensic readiness, such Supplier audit records shall include:

10.2.1 logs to facilitate the identification of the specific asset which makes every outbound request external to the ICT Environment (to the extent it is within the control of the Supplier). To the extent, the design of the ICT Environment allows, such logs shall include those from DHCP servers, HTTP/HTTPS proxy servers, firewalls and routers;

10.2.2 regular reports and alerts giving details of access by users of the ICT Environment (to the extent that it is within the control of the Supplier) to enable the identification of changing access trends any unusual patterns of usage and/or accounts accessing higher than average amounts of Authority Data; and

10.2.3 security events generated in the ICT Environment (to the extent it is within the control of the Supplier) including account logon and logoff events, start and end of remote access sessions, security alerts from desktops and server operating systems and security alerts from third party security software.

10.3 The Parties shall work together to establish any additional audit and monitoring requirements for the ICT Environment.

10.4 The Supplier shall retain audit records collected in compliance with paragraph 10.1 for at least 6 months.

SCHEDULE 7 - PRISONS

[REDACTED DUE TO OPERATIONAL AND COMMERCIAL SENSITIVITY]

SCHEDULE 8 – STATUTORY OBLIGATIONS AND CORPORATE SOCIAL RESPONSIBILITY

1 What the Authority expects from the Supplier

1.1 In September 2017, Her Majesty's Government published a Supplier Code of Conduct (the "**Code**") setting out the standards and behaviours expected of suppliers who work with government. The Code can be found online at:

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/646497/2017-09-3_Official_Sensitive_Supplier_Code_of_Conduct_September_2017.pdf

1.2 The Authority expects the Supplier and its Sub-Contractors to comply with their legal obligations, in particular those set out in Part 1 of this Schedule 8, and to meet the standards set out in the Code as a minimum. The Authority also expects the Supplier and its Sub-Contractors to use reasonable endeavours to comply with the standards set out 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;

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; and

(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, and procure that each of its Sub-Contractors shall, comply with:

(a) the Modern Slavery Act 2015 ("**Slavery Act**"); and

(b) the Authority's anti-slavery policy as provided to the Supplier from time to time ("**Anti-slavery Policy**").

3.2 The Supplier shall:

(a) implement due diligence procedures for its Sub-Contractors and other participants in its supply chains, to ensure that there is no slavery or trafficking in its supply chains;

(b) respond promptly to all slavery and trafficking due diligence questionnaires issued to it by the Authority from time to time and shall ensure that its responses to all such questionnaires are complete and accurate;

(c) 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;

(d) maintain a complete set of records to trace the supply chain of all Services provided to the Authority regarding the Contract; and

(e) implement a system of training for its employees to ensure compliance with the Slavery Act.

3.3 The Supplier represents, warrants and undertakes throughout the Term that:

(a) it conducts its business in a manner consistent with all applicable laws, regulations and codes including the Slavery Act and all analogous legislation in place in any part of the world;

(b) its responses to all slavery and trafficking due diligence questionnaires issued to it by the Authority from time to time are complete and accurate; and

(c) neither the Supplier nor any of its Sub-Contractors, nor any other persons associated with it:

i) has been convicted of any offence involving slavery and trafficking; or

ii) has been or is the subject of any investigation, inquiry or enforcement proceedings by any governmental, administrative or regulatory body regarding any offence regarding slavery and trafficking.

3.4 The Supplier shall notify the Authority as soon as it becomes aware of:

(a) any breach, or potential breach, of the Anti-Slavery Policy; or

(b) any actual or suspected slavery or trafficking in a supply chain which relates to the Contract.

3.5 If the Supplier notifies the Authority pursuant to paragraph 3.4 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.

3.6 If the Supplier is in Default under paragraphs 3.2 or 3.3 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 5.3 of this Schedule 8;

(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; and

(b) keep appropriate records of its compliance with its obligations under paragraph 9.3(a) and make such records available to the Authority on request.

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; and

(b) perform its obligations under the Contract in a way that:

(i) conserves energy, water, wood, paper and other resources;

(ii) reduces waste and avoids the use of ozone depleting substances; and

(iii) minimises the release of greenhouse gases, volatile organic compounds and other substances damaging to health and the environment.

SCHEDULE 9 – DATA PROCESSING

The contact details of the Authority's Data Protection Officer are: **[REDACTED DUE TO OPERATIONAL AND COMMERCIAL SENSITIVITY]**
1.

The contact details of the Supplier's Data Protection Officer are: **[REDACTED DUE TO OPERATIONAL AND COMMERCIAL SENSITIVITY]**

2. The Supplier shall comply with any further written instructions with respect to processing by the Authority.

3. 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]*
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 – BUSINESS CONTINUITY AND DISASTER RECOVERY

1.1 The parties shall comply with the provisions of schedule 10 (Business Continuity and Disaster Recovery) and applicable provisions of schedule 1 (Specification).

1.2 The Supplier shall ensure that it is able to implement the BCDR Plan in accordance with schedule 1 (Specification) and schedule 10 (Business Continuity and Disaster Recovery) at any time in accordance with their terms.

1.3 The Supplier shall undertake regular risk assessments in relation to the provision and maintenance of the Goods not less than once every 12 months and shall provide the results of, and any recommendations in relation to, those risk assessments to the Authority promptly in writing following each review.

1.4 The Supplier shall establish, maintain, and review its own internal processes and procedures with respect to the identification of any threats or risks to the provision of the Goods, how such threats and risks may be mitigated and how the provision of the Goods may be maintained in the event of any such identified threats or risks materialising.

SCHEDULE 11 – FINANCIAL DISTRESS

Version Control

VERSION	DATE	COMMENT
1.0	June 2019	Draft published at ITT stage

1. DEFINITIONS

1.1. In this Schedule, the following definitions shall apply:

"Applicable Financial Indicators" means the financial indicators set out in paragraph 5.1 of this Schedule which are to apply to the Monitored Service Providers as set out in paragraph 5.2 of this Schedule;

"Board" means the Service Provider's board of directors;

"Board Confirmation" means written confirmation from the Board in accordance with Paragraph 8 of this Schedule;

"Financial Distress Event Group" or "FDE Group" means the Service Provider, Key Sub-contractors, the Guarantor and the Monitored Service Providers;

"Financial Indicators" in respect of the Service Provider, Key Sub-contractors and the Guarantor, means each of the financial indicators set out at paragraph 5.1 of this Schedule; and in respect of each Monitored Service Provider, means those Applicable Financial Indicators;

"Financial Target Thresholds" means the target thresholds for each of the Financial Indicators set out at paragraph 5.1 of this Schedule;

"Monitored Service Providers" means those entities specified at paragraph 5.2 of this Schedule;

2. WARRANTIES AND DUTY TO NOTIFY

2.1. The Service Provider warrants and represents to the Authority for the benefit of the Authority that as at the Commencement Date the financial position or, as appropriate, the financial performance of each of the Service Provider, Guarantor and Key Sub-contractors satisfies the Financial Target Thresholds.

2.2. The Service Provider shall:

(a) monitor and report on the Financial Indicators for each entity in the FDE Group against the Financial Target Thresholds on a regular basis and in any event, no less than once a year within 120 calendar days after the Accounting Reference Date; and

(b) promptly notify (or shall procure that its auditors promptly notify) the Authority in writing following the occurrence of a Financial Distress Event or any fact, circumstance or matter which could cause a Financial Distress Event (and in any event, ensure that such notification is made within 10 Working Days of the date on which the Service Provider first becomes aware of the Financial Distress Event or the fact, circumstance or matter which could cause a Financial Distress Event).

2.3. Each report submitted by the Service Provider pursuant to paragraph 2.2(b) shall:

(a) be a single report with separate sections for each of the FDE Group entities;

(b) contain a sufficient level of information to enable the Authority to verify the calculations that have been made in respect of the Financial Indicators;

(c) include key financial and other supporting information (including any accounts data that has been relied on) as separate annexes;

(d) be based on the audited accounts for the date or period on which the Financial Indicator is based or, where the Financial Indicator is not linked to an accounting period or an accounting reference date, on unaudited management accounts prepared in accordance with their normal timetable; and

(e) include a history of the Financial Indicators reported by the Service Provider in graph form to enable the Authority to easily analyse and assess the trends in financial performance.

3. FINANCIAL DISTRESS EVENTS

3.1. The following shall be Financial Distress Events:

(a) an FDE Group entity issuing a profits warning to a stock exchange or making any other public announcement, in each case about a material deterioration in its financial position or prospects;

(b) there being a public investigation into improper financial accounting and reporting, suspected fraud or any other impropriety of an FDE Group entity;

(c) an FDE Group entity committing a material breach of covenant to its lenders;

(d) a Key Sub-contractor notifying the Authority that the Service Provider has not satisfied any material sums properly due under a specified invoice and not subject to a genuine dispute;

(e) any of the following:

(i) commencement of any litigation against an FDE Group entity with respect to financial indebtedness greater than £5m or obligations under a service contract with a total contract value greater than £5m;

(ii) non-payment by an FDE Group entity of any financial indebtedness;

(iii) any financial indebtedness of an FDE Group entity becoming due as a result of an event of default;

(iv) the cancellation or suspension of any financial indebtedness in respect of an FDE Group entity; or

(v) the external auditor of an FDE Group entity expressing a qualified opinion on, or including an emphasis of matter in, its opinion on the statutory accounts of that FDE entity;

in each case which the Authority reasonably believes (or would be likely reasonably to believe) could directly impact on the continued performance and delivery of the Services in accordance with this Contract; and

(f) any one of the Financial Indicators set out at Paragraph 5 for any of the FDE Group entities failing to meet the required Financial Target Threshold.

3.2. The Authority reserves the right to undertake checks by credit rating services to assure itself of the financial viability of any FDE Group entity. Should a credit rating assessment identify concerns in relation to any FDE Group entity, the Authority may consider this to constitute a Financial Distress Event and shall inform the Service Provider of the occurrence of such a Financial Distress Event.

4. CONSEQUENCES OF FINANCIAL DISTRESS EVENTS

4.1. Immediately upon notification by the Service Provider of a Financial Distress Event (or if the Authority becomes aware of a Financial Distress Event without notification and brings the event to the attention of the Service Provider, immediately upon bringing such event to the attention of the Service Provider), the Service Provider shall have the obligations and the Authority shall have the rights and remedies as set out in Paragraphs 4.3 to 4.6.

4.2. In the event of a late or non-payment of a Key Sub-contractor of the type referred to in Paragraph 3.1(d), the Authority shall not exercise any of its rights or remedies under Paragraph 4.3 without first giving the Service Provider 10 Working Days to:

(a) rectify such late or non-payment; or

(b) demonstrate to the Authority's reasonable satisfaction that there is a valid reason for late or non-payment.

4.3. The Service Provider shall (and shall procure that any Monitored Service Provider, the Guarantor and/or any relevant Key Sub-contractor shall):

(a) at the request of the Authority, meet the Authority as soon as reasonably practicable (and in any event within 3 Working Days of the initial notification (or awareness) of the Financial Distress Event or such other period as the Authority may permit and notify to the Service Provider in writing) to review the effect of the Financial Distress Event on the continued performance and delivery of the Services in accordance with this Contract; and

(b) where the Authority reasonably believes (taking into account the discussions and any representations made under Paragraph 4.3(a) that the Financial Distress Event could impact on the continued performance and delivery of the Services in accordance with this Contract:

(i) submit to the Authority for its approval, a draft Financial Distress Remediation Plan as soon as reasonably practicable (and in any event, within 10 Working Days of the initial notification (or awareness) of the Financial Distress Event or such other period as the Authority may permit and notify to the Service Provider in writing); and

(ii) to the extent that it is legally permitted to do so and subject to Paragraph 4.8, provide such information relating to the Service Provider, any Monitored Service Provider, Key Sub-contractors and/or the Guarantor as the Authority may reasonably require in order to understand the risk to the Services, which may include forecasts in relation to cash flow, orders and profits and details of financial measures being considered to mitigate the impact of the Financial Distress Event.

4.4. The Authority shall not withhold its approval of a draft Financial Distress Remediation Plan unreasonably. If the Authority does not approve the draft Financial Distress Remediation Plan, it shall inform the Service Provider of its reasons and the Service Provider shall take those reasons into account in the preparation of a further draft Financial Distress Remediation Plan, which shall be resubmitted to the Authority within 5 Working Days of the rejection of the first draft. This process shall be repeated until the Financial Distress Remediation Plan is approved by the Authority or referred to the dispute resolution procedure under Paragraph 4.5.

4.5. If the Authority considers that the draft Financial Distress Remediation Plan is insufficiently detailed to be properly evaluated, will take too long to complete or will not ensure the continued performance of the Service Provider's obligations in accordance with the Contract, then it may either agree a further time period for the development and agreement of the Financial Distress Remediation Plan or escalate any issues with the draft Financial Distress Remediation Plan using the dispute resolution procedure under clause I1.

4.6. Following Approval of the Financial Distress Remediation Plan by the Authority, the Service Provider shall:

(a) on a regular basis (which shall not be less than fortnightly):

(i) review and make any updates to the Financial Distress Remediation Plan as the Service Provider may deem reasonably necessary and/or as may be reasonably requested by the Authority, so that the plan remains adequate, up

to date and ensures the continued performance and delivery of the Services in accordance with this Contract; and

(ii) provide a written report to the Authority setting out its progress against the Financial Distress Remediation Plan, the reasons for any changes made to the Financial Distress Remediation Plan by the Service Provider and/or the reasons why the Service Provider may have decided not to make any changes;

(b) where updates are made to the Financial Distress Remediation Plan in accordance with Paragraph 4.6(a), submit an updated Financial Distress Remediation Plan to the Authority for its Approval, and the provisions of Paragraphs 4.4 and 4.5 shall apply to the review and approval process for the updated Financial Distress Remediation Plan; and

(c) comply with the Financial Distress Remediation Plan (including any updated Financial Distress Remediation Plan) and ensure that it achieves the financial and performance requirements set out in the Financial Distress Remediation Plan.

4.7. Where the Service Provider reasonably believes that the relevant Financial Distress Event under Paragraph 4.1 (or the circumstance or matter which has caused or otherwise led to it) no longer exists, it shall notify the Authority and the Parties may agree that the Service Provider shall be relieved of its obligations under Paragraph 4.6.

4.8. The Service Provider shall use reasonable endeavours to put in place the necessary measures to ensure that the information specified at paragraph 4.3(b)(ii) is available when required and on request from the Authority and within reasonable timescales. Such measures may include:

(a) obtaining in advance written authority from Key Sub-contractors, the Monitored Service Providers and/or the Guarantor authorising the disclosure of the information to the Authority and/or entering into confidentiality agreements which permit disclosure;

(b) agreeing in advance with the Authority, Key Sub-contractors, the Monitored Service Providers and/or the Guarantor a form of confidentiality agreement to be entered by the relevant parties to enable the disclosure of the information to the Authority;

(c) putting in place any other reasonable arrangements to enable the information to be lawfully disclosed to the Authority (which may include making price sensitive information available to Authority nominated personnel through confidential arrangements, subject to their consent); and

(d) disclosing the information to the fullest extent that it is lawfully entitled to do so, including through the use of redaction, anonymization and any other techniques to permit disclosure of the information without breaching a duty of confidentiality.

5. FINANCIAL INDICATORS

5.1. Subject to the calculation methodology set out at Annex 4 of this Schedule, the Financial Indicators and the corresponding calculations and thresholds used to determine whether a Financial Distress Event has occurred in respect of those Financial Indicators, shall be as follows:

Financial Indicator	Calculation[1]	Financial Target Threshold:
1 Return on capital ratio (%)	Earnings before interest, tax, depreciation and amortization (EBITDA) / Capital employed * 100	>6.35
2 Return on assets ratio (%)	EBITDA / total assets *100	>1.60
3 Pre-tax profit (%) or EBITDA ratio	EBITDA / Sales * 100	>4.20
4 Working capital as a percentage of sales Ratio (%)	Working Capital / Sales * 100	>2.85
5 Profitability	EBITDA	Profit (a loss would indicate a Financial Distress Event)
6 Solvency	Total assets less total liabilities	Positive net assets (negative net assets represent a Financial Distress Event)
7 Gearing	(Long term + short term borrowings) / Shareholder equity * 100	<=30
8 Liquidity	(Current assets – Inventory or stock) / Current Liabilities	>1.0
9 Working capital trade receivables (days)	Average trade debtors / Turnover * 365 days	<33.05
10 Working capital trade payables (days)	Average trade creditors / Cost of sales * 365 days	>6.05
11 Sales per employee	Sales / Number of employees	>109.96
12 Pre-tax profit per employee	EBITDA / Number of employees	>2.29
13 Capital employed per employee	Capital employed / Number of employees	>25.44
Qualified/ Unqualified accounts	Assessment on whether the Authority can place reliance on the provider's financial statements.	Unqualified opinion (qualified opinion, adverse opinion or disclaimer of opinion represents a Financial Distress Event)
Senior personnel involved with insolvency proceedings	Assessment of whether the provider's senior personnel are by law in a position to run the company and whether there is a risk of the company could be wound up.	Senior personnel must not be involved with insolvency proceeding (involvement represents a Financial Distress Event)

Key: [1] – See Annex 4 of this Schedule which sets out the calculation methodology to be used in the calculation of each Financial Indicator.

5.2. Monitored Service Providers

Monitored Service Provider	Applicable Financial Indicators [these are the Financial Indicators from the table at 5.1 which are to apply to the Monitored Service Providers]
[Entity 1 e.g. Group Member, Sub-contractor, Relevant Parent Company etc.]	[1 – Return on Capital Ratio] [2 – etc..] [3][4][5][6][7][8][etc..]
[Entity 2 e.g. Group Member, Sub-contractor, Relevant Parent Company etc.]	[1 – Return on Capital Ratio] [2 – etc..] [3][4][5][6][7][8][etc..]

6. TERMINATION RIGHTS

6.1. The Authority shall be entitled to terminate this Agreement under Clause H4 (Other Termination Grounds) if:

(a) the Provider fails to notify the Authority of a Financial Distress Event in accordance with Paragraph 2.2(b);

(b) the Parties fail to agree a Financial Distress Remediation Plan (or any updated Financial Distress Remediation Plan) in accordance with Paragraphs 4.3 to 4.5; and/or

(c) the Service Provider fails to comply with the terms of the Financial Distress Remediation Plan (or any updated Financial Distress Remediation Plan) in accordance with Paragraph 4.6(c).

7. NOT USED

8. BOARD CONFIRMATION

8.1. If this Contract has been specified as a Critical Service Contract under Paragraph 10.1 of Part 2 to Schedule 15 (Service Continuity Plan and Corporate Resolution Planning) then, **subject to Paragraph 8.4 of this Schedule, the Service Provider shall within 120 calendar days after each Accounting Reference Date or within 15 months of the previous Board Confirmation (whichever is the earlier) provide a Board Confirmation to the Authority in the form set out at Annex 5 of this Schedule, confirming that to the best of the Board's knowledge and belief, it is not aware of and has no knowledge:**

(a) that a Financial Distress Event has occurred since the later of the Commencement Date or the previous Board Confirmation or is subsisting; or

(b) of any matters which have occurred or are subsisting that could reasonably be expected to cause a Financial Distress Event.

8.2. The Service Provider shall ensure that in its preparation of the Board Confirmation it exercises due care and diligence and has made reasonable enquiry of all relevant Staff and other persons as is reasonably necessary to understand and confirm the position.

8.3. In respect of the first Board Confirmation to be provided under this Contract, the Service Provider shall provide the Board Confirmation within 15 months of the Commencement Date if earlier than the timescale for submission set out in Paragraph 8.1 of this Schedule.

8.4. Where the Service Provider is unable to provide a Board Confirmation in accordance with Paragraphs 8.1 to 8.3 of this Schedule due to the occurrence of a Financial Distress Event or knowledge of subsisting matters which could reasonably be expected to cause a Financial Distress Event, it will be sufficient for the Service Provider to submit in place of the Board Confirmation, a statement from the Board of Directors to the Authority (and where the Service Provider is a Strategic Supplier , the Service Provider shall send a copy of the statement to the Cabinet Office Markets and Suppliers Team) setting out full details of any Financial Distress Events that have occurred and/or the matters which could reasonably be expected to cause a Financial Distress Event.

ANNEX 1: NOT USED

ANNEX 2: NOT USED

ANNEX 3: NOT USED

ANNEX 4: CALCULATION METHODOLOGY FOR FINANCIAL INDICATORS

The Service Provider shall ensure that it uses the following general and specific methodologies for calculating the Financial Indicators against the Financial Target Thresholds:

General methodology

1 Terminology: The terms referred to in this Annex are those used by UK companies in their financial statements. Where the entity is not a UK company, the corresponding items should be used even if the terminology is slightly different (for example a charity would refer to a surplus or deficit rather than a profit or loss).

2 Groups: Where the entity is the holding company of a group and prepares consolidated financial statements, the consolidated figures should be used.

3 Foreign currency conversion: Figures denominated in foreign currencies should be converted at the exchange rate in force at the relevant balance sheet date.

4 Treatment of non-underlying items: Financial Indicators should be based on the figures in the financial statements before adjusting for non-underlying items.

Specific Methodology

Financial Indicator	Specific Methodology Or Description
Return on capital (%)	Assessment of provider's profitability and the efficiency with which its capital is employed. EBITDA = Earnings before interest, Tax, Depreciation and Amortisation (EBITDA)
Return on assets (%)	Evaluation of how well management is employing the company's total assets to make a profit. EBITDA = Earnings before interest, Tax, Depreciation and Amortisation (EBITDA)
Pre-tax profit (%)	Assessment of how profitable the provider is. EBITDA = Earnings before interest, Tax, Depreciation and Amortisation (EBITDA)
Working capital as % of sales	Calculation of how much provider spends on operational expenses and short-term debt obligations for every £1 of sales. **Working capital** = current assets / current liabilities or, **Working capital** = (cash + short-term investments + inventory + accounts receivables) / (short-term notes + accounts payables) **Working Capital/Sales*100**
Return on capital employed (%)	Assessment of provider's profitability and the efficiency with which its capital is employed. EBITDA = Earnings before interest, Tax, Depreciation and Amortisation Capital Employed = Total Assets – **Current** liabilities
Profitability (£000)	Assessment of overall profitability. EBITDA = Earnings before interest, Tax, Depreciation and Amortisation

Solvency (£000)	Assessment of available financial resources to deal with adverse trading conditions or legal claims. Solvency = Total Assets – Total Liabilities
Gearing	Assessment on debt used for funding. Long term (over 12 months) + Short term borrowing (repayable within 12 months) / Shareholders equity *100
Liquidity	Assessment of ability to meet short term debts. Where provider has a higher than expected gearing ratio, we will consider other ratios like gearing and profitability to assess Provider's ability to fund its business through existing operations. Current Assets + Inventory or Stock/ Current Liability
Sales per employee (£000)	Measure of how efficiently provider is utilising its employees. Sales or Turnover
Pre-tax profit per employee (£000)	Measure of provider's employees' contribution to organization's profit. Pre-tax profit= = Earnings before interest, Tax, Depreciation and Amortisation
Capital employed per employee (£000)	Measure of capital used to acquire profit per employee.

	Capital Employed = Total Assets – **Current** liability
Qualified/ Unqualified accounts	Assessment on whether the Authority can place reliance on the provider's financial statements.
Senior personnel involved with insolvency proceedings	Assessment of whether the provider's senior personnel are by law in a position to run the company and whether there is a risk of the company could be wound up.

Ministry of Justice

ANNEX 5: BOARD CONFIRMATION

Service Provider Name:

Contract Reference Number:

The Board of Directors acknowledge the requirements set out at paragraph 8 of Schedule 14 (Financial Distress) and confirm that the Service Provider has exercised due care and diligence and made reasonable enquiry of all relevant Staff and other persons as is reasonably necessary to enable the Board to prepare this statement.

The Board of Directors confirms, to the best of its knowledge and belief, that as at the date of this Board Confirmation it is not aware of and has no knowledge:

a) that a Financial Distress Event has occurred since the later of the previous Board Confirmation and the Commencement Date or is subsisting; or

b) of any matters which have occurred or are subsisting that could reasonably be expected to cause a Financial Distress Event.

On behalf of the Board of Directors:

Chair ……

Signed……

Date ……

Director ……

Signed……

Date ……

For the purposes of signature MOJ use a digital solution that may require contract documents to be split into two or more parts. This is to facilitate signature only and has no impact on the formation or management of the contract.

Part two of two.

IN WITNESS of which the 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	
Name	
Position	
Date	

SIGNED for and on behalf of the Assa Abloy Limited	
Name	
Position	
Date	