PART C – PERFORMANCE MANAGEMENT

6. SERVICE LEVEL AGREEMENTS (SLA'S)

6.1 Annex 2 sets out the SLAs which the Parties have agreed shall be used to measure the performance of the Services by the Supplier.

6.2 The Supplier shall monitor its performance against each SLA and shall provide the Authority with a monthly report detailing the level of service actually achieved.

6.3 The Supplier shall implement all measurement and monitoring tools and procedures necessary to measure and report on the Suppliers performance of the Services against the applicable SLAs at a level of detail sufficient to verify compliance with the SLAs.

7. SERVICE CREDITS / DEBITS

7.1 Service Credits / Debits shall be calculated in accordance with the Tables in Annex 2.

7.2 PERFORMANCE MONITORING REPORTS

7.3 Within 7 Days of the end of each Month(by the 7th day of the following month), the Supplier shall deliver to the Authority:

(a) a report which summarises the performance by the Supplier against each SLA; and

7.4 Within 7 Days of the end of each Month (by the 7th day of the following month), the Supplier shall deliver to the Authority a case report setting out a detailed breakdown of its performance against the applicable SLAs during the preceding Month (the "SLA Report").

7.5 The SLA Report shall be in such format as is agreed between the Parties from time to time and shall contain, as a minimum, the following information:

(a) for each SLA, the actual performance achieved over the Month, and that achieved over all previous months of the current financial year;

(b) a summary of all SLA failures that occurred during the relevant Month;

(c) which SLA failures, if any, remain outstanding from previous Months and the steps being taken by the Supplier to resolve them;

(d) the Service Credits / Debits to be applied in respect of each SLA measure;

(e) the details of quality checks undertaken on SLA measures; and

(f) such other details as the Authority may require from time to time.

7.6 The Authority shall review the SLA Report and shall, within 10 Working Days of receipt, notify to the Supplier whether or not it agrees with the Suppliers assessment of the Service Credits / Debits accrued during the Month to which the SLA Report relates.

7.7 If the Authority agrees with the SLA Report, the Authority shall be entitled to apply the Service Credits / Debits.

7.8 If the Authority disagrees with the SLA Report, the Parties shall, no later than 13 Working Days after the notification, meet and seek to agree the level of Service Credits / Debits accrued. Upon agreement of the applicable Service Credits / Debits, the Authority shall be entitled to apply the Service Credits / Debits.

PART D – SERVICE CREDITS / DEBITS

8. SERVICE CREDIT / DEBIT CALCULATION

8.1 Service Credits / Debits are calculated as per the information set out in Annex 2 and Schedule 1 and will be applied from the Commencement Date.

9. INVOICING PROCEDURE

9.1 The Service Credit/Debit will be applied to the validated and agreed invoice value for the Services of the previous Month. Invoices of the previous Month must be agreed and validated before Service Debits/Credits are applied and added to the current invoice.

ANNEX 1 – UNIT CHARGES AND ENFORCEMENT COSTS

TABLE A – UNIT CHARGES

ACTIVITY	UNIT CHARGE
Income Contribution Order (ICO)	[redacted]
Capital & Equity Check (K&E)	
Capital Contribution Order (CCO)	
Appeals	

TABLE B – ENFORCEMENT COSTS

Name	Price
Charging Order – Court Lodging Fee	[redacted]
Charging Order – Court Fees	
Charging Order Fixed Costs	
Charging Order – Disbursements (Solicitors Fee)	
Charging Order – Solicitors Attendance Fee	
Land Registry Fees – Fee to Land Registry to register the Award	
Charging Orders – Admin Copies	
Attachment of Earnings – Court Lodging Fee	
Attachment of Earnings – Court Fees	
Attachment of Earnings – Fixed Costs	
Attachment of Earnings – Solicitors Fee	
High Court Writ – Court Lodging Fee	
High Court Writ – Court Fee	
High Court Writ – Fixed Costs	
High Court Writ – Fixed Court Cost	
Motor Vehicle Clamping	
Third Party Debt Order – Court Lodging Fee	
Third Party Debt Order – Court Fee	
Third Party Debt Order – Fixed Costs	

Third Party Debt Order – Agent Fee	[redacted]

ANNEX 2 – SERVICE LEVEL AGREEMENTS (SLA's) / PERFORMANCE MEASURES

1. **Collection Rate against total debt book value**		
SLA – Target:	**Reporting period**	**Reporting frequency**
Overall % of monies collected or secured as against the monies that were due. a) less than 64.49% **- 2** b) 64.50% - 64.99% **- 1** c) 65.00% - 66.50% **0** d) 66.51% - 67.00% **+1** e) greater than 67.01% **+ 2**	Annually	Monthly
2. **Performance against monthly collection target (%)**		
SLA – Target:	**Reporting period**	**Reporting frequency**
Gross cash and debt secured within the month: a) less than 95% **-2** b) 95.01% - 97.99% **-1** c) 98.00% - 102% **0** d) 102.01% - 110% **+1** e) greater than 110% **+2**	Monthly:	Monthly
3. **Cash collection performance against YTD collection target (%)**		

SLA – Target:	Reporting period	Reporting frequency
Gross cash collections as an accumulative total of total collections: a) less than 64% **-2** b) 64.00% - 66.99% **-1** c) 67.00% - 72.00% **0** d) 72.01% - 75.00% **+1** e) greater than 75.01% **+2**	Annually	Monthly
4. **Performance against annual gross collection target**		
SLA – Target:	**Reporting period**	**Reporting frequency**
Cumulative amount of cash collected and debt secured as against projected collections on the LAA Target Report: a) less than 90% **-2** b) 90.01% - 98.99% **-1** c) 99.00% - 102% **0** d) 102.01% - 115% **+1** e) greater than 115.01% **+2**	Annually	Monthly
5. **Performance against annual secured debt conversion target**		

SLA – Target:	Reporting period	Reporting frequency
Cumulative amount of secured debt converted into paid in cash against LAA gross target: a) less than 85% **-2** b) 85.01% - 97.99% **-1** c) 98.00% - 102% **0** d) 102.01% - 115% **+1** e) greater than 115.01% **+2**	Annually	Monthly
6. **Performance against annual 'Aged Debt' target**		
SLA – Target:	**Reporting period**	**Reporting frequency**
Cumulative amount of aged debt converted into paid in cash against LAA gross target: a) less than 23% **-2** b) 23.01% - 24.99% **-1** c) 25.00% - 29.00% **0** d) 29.01% - 31% **+1** e) greater than 31.01% **+2**	Annually	Monthly
7. **Initial notification letter within 1 working day of account set up**		
SLA – Target:	**Reporting period**	**Reporting frequency**

100% dispatch to Defendant of initial notification letter with 1 Working Day of Defendant Account setup. **+1**	Monthly	Monthly
8. **Defendant reminder within 5 working days following a convicted conclusion at Trial**		
SLA – Target:	**Reporting period**	**Reporting frequency**
Contact 100% of Defendants 5 working days after case outcome received **+1**	Monthly	Monthly
9. **Defendant reminder – 5 days prior to payment due date**		
SLA – Target:	**Reporting period**	**Reporting frequency**
Contact 100% of Defendants 5 days prior to any payment due date. **+1**	Monthly	Monthly
10. **Defendant reminder – 5 working days after overdue payment**		
SLA– Target:	**Reporting period**	**Reporting frequency**
Contact 100% of Defendants a maximum of 5 working days after payment due date if any payments are missed. **+1**	Monthly	Monthly
11. **Dealing with enquiries from the Authority within 5 days**		
SLA – Target:	**Reporting period**	**Reporting frequency**
98% of enquiries from client to be responded to within a maximum of 5 working days. **+1**	Monthly:	Monthly
12. **Dealing with Defendant enquiries within 5 working days**		
SLA – Target:	**Reporting period**	**Reporting frequency**
98% of enquiries from defendant to be responded to within a maximum of 5 Working Days. **+1**	Monthly:	Monthly
13. **Processing of refunds due to the acquitted defendant within 5 working days of notification of acquittal / change**		
SLA – Target:	**Reporting period**	**Reporting frequency**

98% of all refunds due to the defendant to be processed and dispatched within 5 Working Days of receipt of notification of refund being due or authorised. **+1**	Monthly:	Monthly
14. **Management Information within 7 days of month / quarter end and weekly data on next working day**		
SLA – Target:	**Reporting period**	**Reporting frequency**
100% of defined management information be provided by the 7th day of the following month or the next working day if the 7th is a non-working day **+1**	Monthly:	Monthly
15. **Ad Hoc reporting within 7 working days of request**		
SLA – Target:	**Reporting period**	**Reporting frequency**
100% to be provided within 7 working days of the specification for the report being signed and agreed by both parties or, if prioritised by the Client, at an earlier date to be agreed. **+1**	Monthly:	Monthly
16. **Complaints responded within a minimum of 5 working days**		
SLA – Target:	**Reporting period**	**Reporting frequency**
a) 100% of any Complaints received, whether by telephone or in writing, must be recorded. **+1** b) 100% of Complaints must have a substantive response issued within 5 Working Days. **+1** c) 90% of Complaints to be resolved to the satisfaction of the complainant within 10 Working Days. **+1**	Monthly:	Monthly
17. **Completion of Capital and Equity checks**		

SLA – Target:	Reporting period	Reporting frequency
a) 97% of capital and equity checks to be completed within 20 working days of the K&E case being received or the FDC being received. **+1** b) 100% of capital and equity checks to meet the required level of quality **+1**	Monthly:	Monthly
18. **Issue of Capital Contribution Order within 5 days of completion of Capital and Equity check**		
SLA – Target:	**Reporting period**	**Reporting frequency**
a) 95% of Capital Contribution Orders to be issued within 5 working days of the completion of the K&E check or receipt of the FDC amount if a K&E check is not required. **+1** b) 100% of Capital Contribution Orders to be calculated accurately **+1**	Monthly:	Monthly
19. **Defendant Account set up within 1 day (24 hours) of receipt of data file**		
SLA – Target:	**Reporting period**	**Reporting frequency**
100% of Defendant Accounts to be setup within Supplier's Electronic Case Management System (ECMS) within 1 Working Day of receipt of Data File a) 100% **0** b) If less than 100% **-1**	Monthly:	Monthly
20. **Transfer of 100% Collected Contributions to the Authority**		

SLA – Target:	Reporting period	Reporting frequency
100% of cleared funds to be transferred to Client on a weekly basis. a) 100% **0** b) If less than 100% **-1**	Monthly:	Monthly
21. **Remittance data provided to the Authority**		
SLA – Target:	**Reporting period**	**Reporting frequency**
100% of remittance data to be provided to Client on a weekly basis. a) 100% **0** b) If less than 100% **-1**	Monthly	Monthly
22. **Supplier website availability**		
SLA – Target:	**Reporting period**	**Reporting frequency**
Website to be available 95.5% of the time. a) 95.5% - 100% **0** b) If less than 95.5% **-1**	Monthly	Monthly

SCORING KEY

Scoring Key – Collection SLAs (1-6)		
Lower	Upper	Service Credit/Debit
-12	-12	-8.00%
-11	-11	-7.33%
-10	-10	-6.67%
-9	-9	-6.00%
-8	-8	-5.33%
-7	-7	-4.67%
-6	-6	-4.00%
-5	-5	-3.33%
-4	-4	-2.67%
-3	-3	-2.00%
-2	-2	-1.33%
-1	-1	-0.67%
0	0	0.00%
1	1	0.67%
2	2	1.33%
3	3	2.00%
4	4	2.67%
5	5	3.33%

6	6	4.00%
7	7	4.67%
8	8	5.33%
9	9	6.00%
10	10	6.67%
11	11	7.33%
12	12	8.00%

Scoring Key – Admin SLAs (7-22)		
Lower	Upper	Service Credit/Debit
-4	9	-2%
10	12	-1%
13	13	0%
14	14	1%
15	16	2%

SCHEDULE 3 - CHANGE CONTROL

Contract Change Notice ("CCN")

CCN: **Contract Reference Number & Title** **Change Title**	

WHEREAS the Supplier and the Authority entered into a Contract for the supply of Debt Collection and Enforcement Services dated [dd/mm/yyyy] (the "**Original Contract**") and now wish to amend the Original Contract

IT IS AGREED as follows

1. The Original Contract shall be amended as set out in this CCN:

Change Requestor / Originator		
Summary of Change		
Reason for Change		
Revised Contract Price	Original Contract Value	£
	Previous Contract Changes	£
	Contract Change Note [x]	£
	New Contract Value	£
Revised Payment Schedule		
Revised Specification (See Annexe [x] for Details) *[Note: any change to the Specification should be added as an Annex to the CCN]*		
Revised Contract Period		
Change in Contract Manager(s)		
Other Changes		

2. Save as amended in the CCN all other terms of the Original Contract remain effective.

3. The CCN takes effect from the date on which both Parties sign below.

IN WITNESS of which this CCN has been duly executed by the Parties.

SIGNED for and on behalf of the Secretary of State for Justice
Signature:
Name (block capitals):
Position:
Date:

SIGNED for and on behalf of [insert name of Supplier]
Signature:
Name (block capitals):
Position:
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
1.8.8 FVRA template	15/05/2018	A period of six years from duration of the contract end date, and subject to written consent from Marston Holdings.
5.1 Monthly management reports	15/05/2018	A period of six years from duration of the contract end date, and subject to written consent from Marston Holdings.
6.1 Gantt chart	15/05/2018	A period of six years from duration of the contract end date, and subject to written consent from Marston Holdings.
Annex K – LAA cost model	15/05/2018	A period of six years from duration of the contract end date, and subject to written consent from Marston Holdings.
Annex B – subcontractor info	15/05/2018	A period of six years from duration of the contract end date, and subject

		to written consent from Marston Holdings.

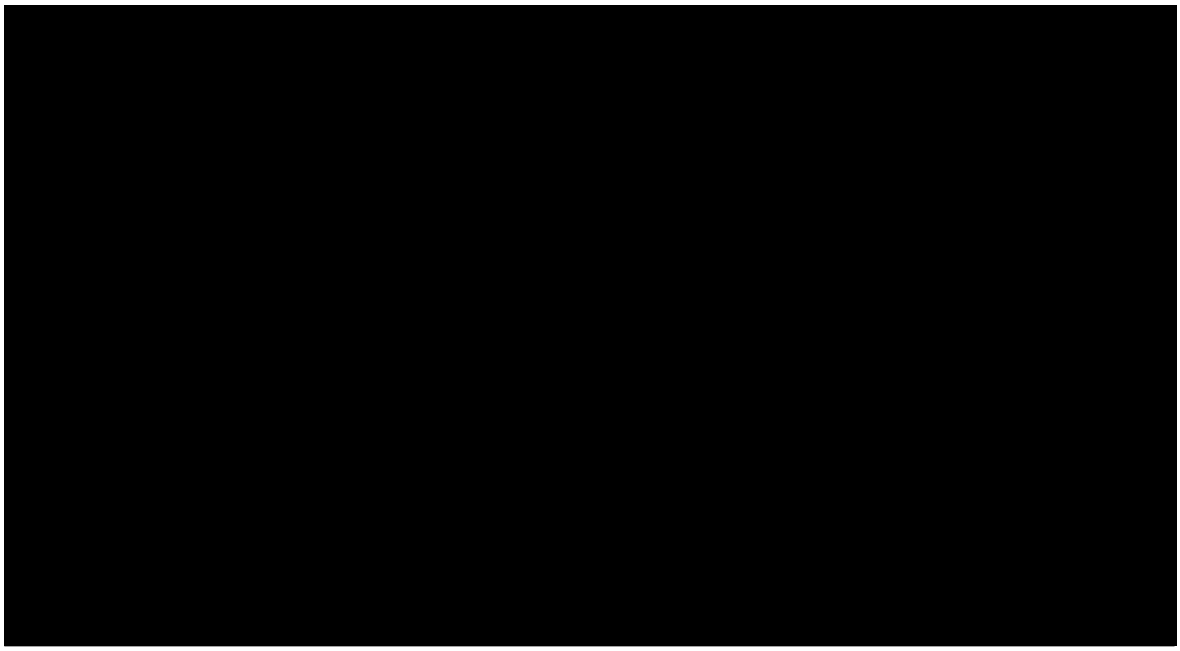
SCHEDULE 5 – SUPPLIER AND THIRD PARTY SOFTWARE

Supplier Software comprises the following:

Software	Supplier (if Affiliate of the Supplier)	Purpose	No. of Licences	Restrictions	No. of copies	Other	To be deposited in escrow?
[redacted]							

Third Party Software comprises the following:

Third Party Software	Supplier	Purpose	No. of Licences	Restrictions	No. of copies	Other	To be deposited in escrow?
[redacted]							



SCHEDULE 6 – INFORMATION ASSURANCE AND 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 B4 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.

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:

(a) has been tested; and

(b) 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);

(a) 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;

(b) provide a level of security which ensures that the ISMS and the Supplier System:

(i) meet the requirements in the Contract;

(ii) are in accordance with applicable Law;

(iii) 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;

(iv) comply with the Security Policy Framework and any other relevant Government security standards;

(v) comply with the Baseline Security Requirements;

(vi) comply with the Authority's policies, including, where applicable, the Authority's Information Assurance Policy in PSI 24/2014;

(c) address any issues of incompatibility with the Supplier's organisational security policies;

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

(e) document:

(i) 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;

(ii) incident response plans, including the role of nominated security incident response companies; and

(iii) 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 security patches and the reporting and audit mechanism detailing the efficacy of the patching policy;

(f) 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

(g) be certified by (or by a person with the direct delegated authority of) the Suppliers 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 Contract Period 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:

(a) comply with the Baseline Security Requirements;

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

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

(d) 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;

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

(f) set out the scope of the Authority System that is under the control of the Supplier;

(g) be structured in accordance with ISO/IEC 27001: 2013 or equivalent unless otherwise Approved; and

(h) 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; and

(i) 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 Contract Period 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.

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 Contract Period (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:

(a) any issues in implementing the Security Policy Framework and/or managing information risk;

(b) emerging changes in Good Industry Practice;

(c) any proposed or actual change to the ICT Environment and/or associated processes;

(d) any new perceived, potential or actual security risks or vulnerabilities;

(e) any ISO27001: 2013 audit report or equivalent produced in connection with the Certification Requirements which indicates concerns; and

(f) 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:

(a) suggested improvements to the effectiveness of the ISMS, including controls;

(b) updates to risk assessments; and

(c) 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 F9 (Variation) 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 F9, the Parties shall thereafter follow clause F9 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:

(a) 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

(b) the Government's Cyber Essentials Scheme at the BASIC level unless otherwise agreed with the Authority

and shall provide the Authority with evidence:

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

(d) 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 Contract Term.

5.2 The Supplier shall ensure that it:

(a) 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

(b) 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:

(a) immediately cease access to and use of Information Assets and/or Authority Data; and

(b) 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 Contract Period, which shall include:

(a) 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;

(b) an annual IT Health Check by an independent CHECK 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;

(c) 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

(d) such other tests as are required:

(i) by any Vulnerability Correction Plans;

(ii) by ISO/IEC 27001:2013 certification requirements or equivalent Approved;

(iii) after any significant architectural changes to the ICT Environment;

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

(v) following a Breach of Security.

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

(a) agree with the Authority the aim and scope of the IT Health Check;

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

(c) in the event that the IT Health Check report identifies any vulnerabilities:

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

(ii) how the vulnerability will be remedied;

(iii) the date by which the vulnerability will be remedied;

(iv) 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;

(v) comply with the Vulnerability Correction Plan; and

(vi) 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 so as 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:

(a) upon giving reasonable notice to the Supplier where reasonably practicable to do so; and

(b) 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(a) or 6.5(b), 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:

(a) vulnerabilities during any accreditation process, the Supplier shall track and resolve them effectively; and

(b) 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:

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

(b) 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:

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

(b) 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 independently audited in accordance with ISO/IEC 27001: 2013 or equivalent. The Authority and its authorised representatives shall, where applicable, be granted access to the Supplier premises 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 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 if applicable, upon becoming aware of any Breach of Security or attempted Breach of Security, the Supplier shall:

(a) 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:

(i) minimise the extent of actual or potential harm caused by any Breach of Security;

(ii) 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;

(iii) mitigate against a Breach of Security or attempted Breach of Security; and

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

(b) 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

(c) 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, 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:

(a) functions in accordance with Good Industry Practice for protecting external connections to the internet;

(b) functions in accordance with Good Industry Practice for protection from malicious code;

(c) 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;

(d) is patched (and all of 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

(e) 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:

(a) 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

(b) 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:

(a) 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;

(b) 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

(c) 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 Contract Period within 6 months of the release of the latest version unless:

(a) 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

(b) otherwise agreed with the Authority in writing.

9.5 The Supplier shall:

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

(b) 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;

(c) 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 Contract Term;

(d) 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;

(e) from the Commencement Date and within 5 Working Days of the end of each subsequent month during the Contract Period 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;

(f) 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;

(g) 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

(h) 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.

ANNEX 1

BASELINE SECURITY REQUIREMENTS

1. SECURITY CLASSIFICATIONS AND CONTROLS

1.1 The Supplier shall, unless otherwise Approved in accordance with paragraph 7.2 of this Annex 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 minimum 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:

(a) 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;

(b) 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:

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

(b) 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;

(c) protected by an authentication mechanism, such as a password; and

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

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 Laws. 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:

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

(b) 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:

(a) protects the confidentiality of the Authority during transfer through encryption suitable for the impact level of the data;

(b) 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

(c) prevents the repudiation of receipt through accounting and auditing.

3.6 The Supplier shall:

(a) protect Authority Data, including sensitive 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;

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

(c) on demand, provide the Authority with all Authority Data in an agreed open format;

(d) have documented processes to guarantee availability of Authority Data if it ceases to trade;

(e) 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;

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

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

(i) destroy paper records containing protected Personal Data by incineration, pulping or shredding so that reconstruction is unlikely; and

(ii) dispose of electronic media that has been used for the processing or storage of protected 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.