Schedule 2.4 – Contract Security Management

1 **Definitions**

1.1 In this Schedule, the following definitions shall apply:

Breach of Security	the occurrence of: a) any unauthorised access to or use of the Services, the Authority Premises, the Sites, the Supplier System, the Authority System (to the extent that it is under the control of the Supplier) and/or any IT, information or data (including the Confidential Information and the Authority Data) used by the Authority and/or the Supplier in connection with this Agreement; and/or b) the loss and/or unauthorised disclosure of any information or data (including the Confidential Information and the Authority Data), including any copies of such information or data, used by the Authority and/or the Supplier in connection with this Agreement, in either case as more particularly set out in the Security requirements in the Statement of Requirements and the Baseline Security Requirements;
ISMS	the information security management system and processes developed by the Supplier in accordance with Paragraph 3 as updated from time to time in accordance with this Schedule;
Security Tests	tests to validate the ISMS and security of all relevant processes, systems, incident response plans, patches to vulnerabilities and mitigations to Breaches of Security.

2 **Introduction**

2.1 The Parties acknowledge that the purpose of the ISMS and Security Management Plan are to ensure a good organisational approach to security under which the specific requirements of this Agreement will be met. This Schedule is supplemental to the Statement of Requirements. If the Supplier becomes aware of any conflict between the requirements of this Schedule and any element of the Statement of Requirements the Supplier shall notify the Authority Representative immediately of such conflict and the Authority Representative shall, as soon as practicable, notify the Supplier which provision the Supplier shall comply with.

2.2 The Parties shall each appoint a member of the OPR Group to be responsible for security. The initial member of the OPR Group appointed by the Supplier for such purpose shall be the person named as such in Schedule 9.2 (Key Personnel) and the provisions of Clauses 14.5 and 14.6 (Key Personnel) shall apply in relation to such person.

2.3 The Authority shall clearly articulate its high level security requirements so that the Supplier can ensure that the ISMS, security related activities and any mitigations are driven by these fundamental needs.

2.4 Both Parties shall provide a reasonable level of access to any members of their personnel for the purposes of designing, implementing and managing security.

2.5 The Supplier shall use as a minimum Good Industry Practice in the day to day operation of any system holding, transferring or processing Authority Data and any system that could directly or indirectly have an impact on that information, and shall ensure that Authority Data remains under the effective control of the Supplier at all times.

2.6 The Supplier shall ensure the up-to-date maintenance of a security policy relating to the operation of its own organisation and systems and on request shall supply this document as soon as practicable to the Authority.

2.7 The Authority and the Supplier acknowledge that information security risks are shared between the Parties and that a compromise of either the Supplier or the Authority's security provisions represents an unacceptable risk to the Authority requiring immediate communication and co-operation between the Parties.

3 ISMS

3.1 By the date specified in the Implementation Plan the Supplier shall develop and submit to the Authority for the Authority's approval in accordance with Paragraph 4.4 an ISMS (information security management system) for the purposes of this Agreement, which:

3.1.1 shall have been tested in accordance with Schedule 6.2 (Testing); and

3.1.2 shall comply with the requirements of Paragraphs 3.3 to 3.5.

3.2 The Supplier acknowledges that the Authority places great emphasis on the reliability of the Services and confidentiality, integrity and availability of information and consequently on the security provided by the ISMS and that it shall be responsible for the effective performance of the ISMS.

3.3 3.3 The ISMS shall:

3.3.1 unless otherwise specified by the Authority in writing, be developed to protect all aspects of the Services and all processes associated with the delivery of the Services, including the Authority Premises, the Sites, the Supplier System, the Authority System (to the extent that it is under the control of the Supplier) and any IT, information and data (including the Authority Confidential Information and the Authority Data) to the extent used by the Authority or the Supplier in connection with this Agreement;

3.3.2 meet the relevant standards in ISO/IEC 27001 and ISO/IEC 27002 in accordance with Paragraph 7; and

3.3.3 at all times provide a level of security which:

a) is in accordance with Law and this Agreement;

b) as a minimum demonstrates Good Industry Practice;

c) complies with the Baseline Security Requirements;

d) addresses issues of incompatibility with the Supplier's own organisational security policies;

e) meets any specific security threats of immediate relevance to the Services and/or Authority Data;

f) complies with the security requirements as set out in the Statement of Requirements; and

g) complies with the Authority's IT policies;

3.3.4 document the security incident management processes and incident response plans;

3.3.5 document the vulnerability management policy including processes for identification of system vulnerabilities and assessment of the potential impact on the Services of any new threat, vulnerability or exploitation technique of which the Supplier becomes aware, prioritisation of security patches, testing of security patches, application of security patches, a process for Authority approvals of exceptions, and the reporting and audit mechanism detailing the efficacy of the patching policy; and

3.3.6 be certified by (or by a person with the direct delegated authority of) a Supplier's main board representative, being the Chief Security Officer, Chief Information Officer, Chief Technical Officer or Chief Financial Officer (or equivalent as agreed in writing by the Authority in advance of issue of the relevant Security Management Plan).

3.4 Subject to Clause 20 (Authority Data and Security Requirements) the references to standards, guidance and policies set out in Paragraph 3.3 shall be deemed to be references to such items as developed and updated and to any successor to or replacement for such standards, guidance and policies, as notified to the Supplier from time to time.

3.5 In the event that the Supplier becomes aware of any inconsistency in the provisions of the standards, guidance and policies set out in Paragraph 3.3, the Supplier shall immediately notify the Authority Representative of such inconsistency and the Authority Representative shall, as soon as practicable, notify the Supplier which provision the Supplier shall comply with.

3.6 If the ISMS submitted to the Authority pursuant to Paragraph 3.1 is approved by the Authority, it shall be adopted by the Supplier immediately and thereafter operated and maintained in accordance with this Schedule. If the ISMS is not approved by the Authority, 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 Parties shall use all reasonable endeavours to ensure that the approval process takes as little time as possible and in any event no longer than 15 Working Days (or such other period as the Parties may agree in writing) from the date of its first submission to the Authority. If the Authority does not approve the ISMS following its resubmission, the matter shall be resolved in accordance with the Dispute Resolution Procedure. No approval to be given by the Authority pursuant to this Paragraph 3 may be unreasonably withheld or delayed. However any failure to approve the ISMS on the grounds that it does not comply with any of the requirements set out in Paragraphs 3.3 to 3.5 shall be deemed to be reasonable.

3.7 Approval by the Authority of the ISMS pursuant to Paragraph 3.6 or of any change to the ISMS shall not relieve the Supplier of its obligations under this Schedule.

4 Security Management Plan

4.1 Within 60 Working Days after the Effective Date, the Supplier shall prepare and submit to the Authority for approval in accordance with Paragraph 4.3 a fully developed, complete and up-to-date Security Management Plan which shall comply with the requirements of Paragraph 4.2.

4.2 The Security Management Plan shall:

4.2.1 be based on the initial Security Management Plan set out in Annex 2;

4.2.2 comply with the Baseline Security Requirements;

4.2.3 identify the necessary delegated organisational roles defined for those responsible for ensuring this Schedule is complied with by the Supplier;

4.2.4 detail the process for managing any security risks from Subcontractors and third parties authorised by the Authority with access to the Services, processes associated with the delivery of the Services, the Authority Premises, the Sites, the Supplier System, the Authority System (to extent that it is under the control of the Supplier) and any IT, Information and data (including the Authority

Confidential Information and the Authority Data) and any system that could directly or indirectly have an impact on that Information, data and/or the Services;

4.2.5 unless otherwise specified by the Authority in writing, be developed to protect all aspects of the Services and all processes associated with the delivery of the Services, including the Affected Properties, the Sites, the Supplier System, the Authority System (to the extent that it is under the control of the Supplier) and any IT, Information and data (including the Authority Confidential Information and the Authority Data) to the extent used by the Authority or the Supplier in connection with this Agreement or in connection with any system that could directly or indirectly have an impact on that Information, data and/or the Services;

4.2.6 set out the security measures to be implemented and maintained by the Supplier in relation to all aspects of the Services and all processes associated with the delivery of the Services and at all times comply with and specify security measures and procedures which are sufficient to ensure that the Services comply with the provisions of this Schedule (including the requirements set out in Paragraph 3.4);

4.2.7 demonstrate that the Detailed Solutions have minimised the Authority and Supplier effort required to comply with this Schedule through consideration of available, appropriate and practicable pan-government accredited services (for example, **platform as a service** offerings from the G-Cloud catalogue);

4.2.8 set out the plans for transiting all security arrangements and responsibilities from those in place at the Effective Date to those incorporated in the ISMS at the date set out in Schedule 6.1 (Implementation Plan and Implementation Phase) for the Supplier to meet the full obligations of the security requirements set out in the Statements of Requirements and this Schedule;

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

4.2.10 be structured in accordance with ISO/IEC 27001 and ISO/IEC 27002, cross-referencing if necessary to other Schedules which cover specific areas included within those standards; and

4.2.11 be written in plain English in language which is readily comprehensible to the staff of the Supplier and the Authority engaged in the Services and shall reference only documents which are in the possession of the Parties or whose location is otherwise specified in this Schedule.

4.3 If the Security Management Plan submitted to the Authority pursuant to Paragraph 4.1 is approved by the Authority, it shall be adopted by the Supplier immediately and thereafter operated and maintained in accordance with this Schedule. If the Security Management Plan is not approved by the Authority, 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 Parties shall use all reasonable endeavours to ensure that the approval process takes as little time as possible and in any event no longer than 15 Working Days (or such other period as the Parties may agree in writing) from the date of its first submission to the Authority. If the Authority does not approve the Security Management Plan following its resubmission, the matter shall be resolved in accordance with the Dispute Resolution Procedure. No approval to be given by the Authority pursuant to this Paragraph 4.3 may be unreasonably withheld or delayed. However any failure to approve the Security Management Plan on the grounds that it does not comply with the requirements set out in Paragraph 4.2 shall be deemed to be reasonable.

4.4 Approval by the Authority of the Security Management Plan pursuant to Paragraph 4.3 or of any change or amendment to the Security Management Plan shall not relieve the Supplier of its obligations under this Schedule.

5 Amendment and Revision of the ISMS and Security Management Plan

5.1 The ISMS and Security Management Plan shall be fully reviewed and updated by the Supplier at least annually to reflect:

5.1.1 emerging changes in Good Industry Practice;

5.1.2 any change or proposed change to the IT Environment, the Services and/or associated processes;

5.1.3 any new perceived or changed security threats; and

5.1.4 any reasonable change in requirement requested by the Authority.

5.2 The Supplier shall provide the Authority with the results of such reviews as soon as reasonably practicable after their completion and amend the ISMS and Security Management Plan at no additional cost to the Authority. The results of the review shall include, without limitation:

5.2.1 suggested improvements to the effectiveness of the ISMS;

5.2.2 updates to the risk assessments carried out in relation to the development of the ISMS and Security Management Plan;

5.2.3 proposed modifications to respond to events that may impact on the ISMS including the security incident management process, incident response plans and general procedures and controls that affect information security; and

5.2.4 suggested improvements in measuring the effectiveness of controls.

5.3 Subject to Paragraph 5.4, any change which the Supplier proposes to make to the ISMS or Security Management Plan (as a result of a review carried out pursuant to Paragraph 5.1, an Authority request, a change to the Statement of Requirements or otherwise) shall be subject to the Change Control Procedure and shall not be implemented until approved in writing by the Authority.

5.4 The Authority may, where it is reasonable to do so, approve and require changes or amendments to the ISMS or Security Management Plan to be implemented on timescales faster than set out in the Change Control Procedure but, without prejudice to their effectiveness, all such changes and amendments shall thereafter be subject to the Change Control Procedure for the purposes of formalising and documenting the relevant change or amendment for the purposes of this Agreement.

6 Security Testing

6.1 The Supplier shall conduct relevant Security Tests from time to time (and at least annually across the scope of the ISMS) and additionally after significant architectural changes to the IT Environment or after any change or amendment to the ISMS, (including security incident management processes and incident response plans) or the Security Management Plan. Security Tests shall be designed and implemented by the Supplier so as to minimise the impact on the delivery of the Services and the date, timing, content and conduct of such Security Tests shall be agreed in advance with the Authority. Subject to compliance by the Supplier with the foregoing requirements, if any Security Tests adversely affect the Supplier's ability to deliver the Services so as to meet the Target Performance Levels, the Supplier shall be granted relief against any resultant under-performance for the period of the Security Tests.

6.2 The Authority shall be entitled to send a representative to witness the conduct of the Security Tests. The Supplier shall provide the Authority with the results of such tests (in a form approved by the Authority in advance) as soon as practicable after completion of each Security Test.

6.3 Without prejudice to any other right of audit or access granted to the Authority pursuant to this Agreement, the Authority and/or its authorised representatives shall be entitled, at any time upon giving reasonable notice to the Supplier, to carry out such tests (including penetration tests) as it may deem necessary in relation to the ISMS (and the Supplier's compliance with the ISMS), the Security Management Plan, the Security Systems and any other aspect of the Services. The Authority may notify the Supplier of the results of such tests after completion of

each such test. If any such Authority test adversely affects the Supplier's ability to deliver the Services so as to meet the Target Performance Levels, the Supplier shall be granted relief against any resultant under- performance for the period of the Authority test.

6.4 Where any Security Test carried out pursuant to Paragraphs 6.2 or 6.3 reveals any actual or potential Breach of Security or weaknesses (including un-patched vulnerabilities, poor configuration and/or incorrect system management), the Supplier shall promptly notify the Authority of any changes to the ISMS and to the Security Management Plan (and the implementation thereof) which the Supplier proposes to make in order to correct such failure or weakness. Subject to the Authority's prior written approval, the Supplier shall implement such changes to the ISMS and the Security Management Plan and repeat the relevant Security Tests in accordance with the timetable agreed with the Authority or, otherwise, as soon as reasonably possible. For the avoidance of doubt, where the change to the ISMS or Security Management Plan is to address a non-compliance with the Baseline Security Requirements or security requirements (as set out in the Statement of Requirements) or the requirements of this Schedule, the change to the ISMS or Security Management Plan shall be at no cost to the Authority.

6.5 If any repeat Security Test carried out pursuant to Paragraph 6.4 reveals an actual or potential Breach of Security exploiting the same root cause failure, such circumstance shall constitute a material Default for the purposes of Clause 27.1 (Rectification Plan Process).

7 ISMS Compliance

7.1 The Authority shall be entitled to carry out such security audits as it may reasonably deem necessary in order to ensure that the ISMS maintains compliance with the principles and practices of ISO 27001, the specific security requirements set out in the Statement of Requirements and the Baseline Security Requirements.

7.2 If, on the basis of evidence provided by such audits, it is the Authority's reasonable opinion that compliance with the principles and practices of ISO/IEC 27001, the specific security requirements set out in the Statement of Requirements and/or the Baseline Security Requirements is not being achieved by the Supplier, then the Authority shall notify the Supplier of the same and give the Supplier a reasonable time (having regard to the extent and criticality of any non-compliance and any other relevant circumstances) to implement any necessary remedy. If the Supplier does not become compliant within the required time then the Authority shall have the right to obtain an independent audit against these standards in whole or in part.

7.3 If, as a result of any such independent audit as described in Paragraph 7.2 the Supplier is found to be non-compliant with the principles and practices of ISO/IEC 27001, the specific security requirements set out in the Statement of Requirements and/or the Baseline Security Requirements then the Supplier shall, at its own expense, undertake those actions required in order to achieve the necessary compliance and shall reimburse in full the costs incurred by the Authority in obtaining such audit.

8 Breach of Security

8.1 Either Party shall notify the other in accordance with the agreed security incident management process as defined by the ISMS upon becoming aware of any Breach of Security or attempted Breach of Security.

8.2 Without prejudice to the security incident management process, upon becoming aware of any of the circumstances referred to in Paragraph 8.1, the Supplier shall:

8.2.1 immediately take all reasonable steps (which shall include any action or changes reasonably required by the Authority) necessary to:

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

b) remedy such Breach of Security to the extent possible and protect the integrity of the IT Environment to the extent within its control against any such Breach of Security or attempted Breach of Security;

c) apply a tested mitigation against any such Breach of Security or attempted Breach of Security and, provided that reasonable testing has been undertaken by the Supplier, if the mitigation adversely affects the Supplier's ability to deliver the Services so as to meet the Target Performance Levels, the Supplier shall be granted relief against any resultant under-performance for such period as the Authority, acting reasonably, may specify by written notice to the Supplier;

d) prevent a further Breach of Security or attempted Breach of Security in the future exploiting the same root cause failure; and

e) supply any requested data to the Authority or the Computer Emergency Response Team for UK Government (**GovCertUK**) on the Authority's request within 2 Working Days and without charge (where such requests are reasonably related to a possible incident or compromise); and

8.2.2 as soon as reasonably practicable 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 where required by the Authority.

8.3 In the event that any action is taken in response to a Breach of Security or potential or attempted Breach of Security that demonstrates non-compliance of the ISMS with the Baseline Security Requirements or security requirements (as set out in the Statement of Requirements) or the requirements of this Schedule, then any required change to the ISMS shall be at no cost to the Authority.

9 Vulnerabilities and Corrective Action

9.1 The Authority and the Supplier acknowledge that from time to time vulnerabilities in the IT Environment will be discovered which unless mitigated will present an unacceptable risk to the Authority's Information.

9.2 The severity of threat vulnerabilities for Supplier COTS Software and Third Party COTS Software shall be categorised by the Supplier as **Critical**, **Important** and **Other** by aligning these categories to the vulnerability scoring according to the agreed method in the ISMS and using the appropriate vulnerability scoring systems including:

9.2.1 the **National Vulnerability Database Vulnerability Severity Ratings**: **High**, **Medium** and **Low** respectively (these in turn are aligned to CVSS scores as set out by NIST http://nvd.nist.gov/cvss.cfm); and

9.2.2 Microsoft's **Security Bulletin Severity Rating System** ratings **Critical**, **Important**, and the two remaining levels (**Moderate** and **Low**) respectively.

9.3 The Supplier shall procure the application of security patches to vulnerabilities within a maximum period from the public release of such patches with those vulnerabilities categorised as **Critical** within 14 days of release, **Important** within 30 days of release and all **Other** within 60 Working Days of release, except where:

9.3.1 the Supplier can demonstrate that a vulnerability is not exploitable within the context of any Service (e.g. because it resides in a software component which is not running in the service) provided vulnerabilities which the Supplier asserts cannot be exploited within the context of a Service must be remedied by the Supplier within the above timescales if the vulnerability becomes exploitable within the context of the Service;

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

9.3.3 the Authority agrees a different maximum period after a case-by-case consultation with the Supplier under the processes defined in the ISMS.

9.4 The Relevant Detailed Solutions and the Implementation Plan shall include provisions for major version upgrades of all Supplier COTS Software and Third Party COTS Software to be upgraded within 6 months of the release of the latest version, such that it is no more than one major version level below the latest release (normally codified as running software no older than the **n-1 version**) throughout the Term unless:

9.4.1 where upgrading such Supplier COTS Software and Third Party COTS Software reduces the level of mitigations for known threats, vulnerabilities or exploitation techniques, provided always that such upgrade is made within 12 months of release of the latest version; or

9.4.2 is agreed with the Authority in writing.

9.5 The Supplier shall:

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

9.5.2 ensure that the IT Environment (to the extent that the IT Environment 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 it is knowledgeable about the latest trends in threat, vulnerability and exploitation that are relevant to the IT Environment by actively monitoring the threat landscape during the Term;

9.5.4 pro-actively scan the IT Environment (to the extent that the IT Environment is within the control of the Supplier) for vulnerable components and address discovered vulnerabilities through the processes described in the ISMS as developed under Paragraph 3.3.5;

9.5.5 from the date specified in the Security Management Plan (and before the first Operational Service Commencement Date) provide a report to the Authority within 5 Working Days of the end of each month detailing both patched and outstanding vulnerabilities in the IT Environment (to the extent that the IT Environment is within the control of the Supplier) and any elapsed time between the public release date of patches and either time of application or for outstanding vulnerabilities the time of issue of such report;

9.5.6 propose interim mitigation measures to vulnerabilities in the IT Environment 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 not needed for the provision of the Services (in order to reduce the attack surface of the Supplier Solution and IT Environment); 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 and provide initial indications of possible mitigations.

9.6 If the Supplier is unlikely to be able to mitigate the vulnerability within the timescales under Paragraph 9, the Supplier shall immediately notify the Authority.

9.7 A failure to comply with Paragraph 9.3 shall constitute a Notifiable Default, and the Supplier shall comply with the Rectification Plan Process.

Annex 1 - Baseline Security Requirements

Higher Classifications

1 The Supplier shall not handle Authority information classified SECRET or TOP SECRET except if there is a specific requirement and in this case prior to receipt of such information the Supplier shall seek additional specific guidance from the Authority.

End User Devices

2 When Authority data resides on a mobile, removable or physically uncontrolled device it must be stored encrypted using a product or system component which has been formally assured through a recognised certification process of the UK Government Communications Electronics Security Group (CESG) to at least Foundation Grade, for example, under the CESG Commercial Product Assurance scheme (CPA).

3 Devices used to access or manage Authority data and services must be under the management authority of Authority or Supplier and have a minimum set of security policy configuration enforced. These devices must be placed into a known good state prior to being provisioned into the management authority of the Authority. Unless otherwise agreed with the Authority in writing, all Supplier devices are expected to meet the set of security requirements set out in the CESG End User Devices Platform Security Guidance (https://www.gov.uk/government/collections/end-user-devices-security-guidance- -2). Where the 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. Where the Supplier wishes to deviate from the CESG guidance, then this should be agreed in writing on a case by case basis with the Authority.

Data Processing, Storage, Management and Destruction

4 The Supplier and Authority recognise the need for the Authority's information to be safeguarded under the UK Data Protection regime or a similar regime. To that end, the Supplier must be able to state to the Authority the physical locations in which data may be stored, processed and managed from, and what legal and regulatory frameworks Authority information will be subject to at all times.

5 The Supplier shall agree any change in location of data storage, processing and administration with the Authority in advance where the proposed location is outside the UK. Such approval shall not be unreasonably withheld or delayed unless specified otherwise in this Agreement and provided that storage, processing and management of any Authority information is only carried out offshore within:

5.1 the European Economic Area (EEA);

5.2 in the US if the Supplier and or any relevant Subcontractor have signed up to the US-EU Privacy Shield;

5.3 or in 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 EU Commission.

6 The Supplier shall:

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

6.2 have documented processes to guarantee availability of Authority Data in the event of the Supplier ceasing to trade;

6.3 securely destroy all media that has held Authority Data at the end of life of that media in line with Good Industry Practice; and

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

7 Networking

7.1 The Authority requires that any Authority Data transmitted over any public network (including the Internet, mobile networks or un-protected enterprise network) or to a mobile device must 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 pan- government accredited encrypted networking services via the Public Sector Network (PSN) framework (which makes use of Foundation Grade certified products).

7.2 The Authority requires that the configuration and use of all networking equipment to provide the Services, including those that are located in secure physical locations, are at least compliant with Good Industry Practice.

8 Security Architectures

8.1 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 IT systems which will process or store Authority Data.

8.2 When designing and configuring the IT Environment (to the extent that the IT Environment 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 a CESG Certified Professional certification (http://www.cesg.gov.uk/awarenesstraining/IA-certification/Pages/index.aspx) for all bespoke or complex components of the Detailed Solutions.

9 Personnel Security

9.1 Supplier Personnel shall be subject to pre-employment checks that include, as a minimum: identity, unspent criminal convictions and right to work.

9.2 The Supplier shall agree on a case by case basis Supplier Personnel roles which require specific government clearances (such as SC) including system administrators with privileged access to IT systems which store or process Authority Data.

9.3 The Supplier shall prevent Supplier Personnel who are unable to obtain the required security clearances from accessing systems which store, process, or are used to manage Authority Data except where agreed with the Authority in writing.

9.4 All Supplier Personnel that have the ability to access Authority Data or systems holding Authority Data shall undergo regular training on secure information management principles. Unless otherwise agreed with the Authority in writing, this training must be undertaken annually.

9.5 Where the Supplier or Sub-Contractors grants increased IT privileges or access rights to Supplier Personnel, those Supplier Personnel shall be granted only those permissions necessary for them to carry out their duties. When staff no longer need elevated privileges or leave the organisation, their access rights shall be revoked within 1 Working Day.

10 Identity, Authentication and Access Control

10.1 The Supplier shall operate an access control regime to ensure all users and administrators of the Supplier Solution are uniquely identified and authenticated when accessing or

administering the Services. Applying the principle of least privilege, users and administrators shall be allowed access only to those parts of the Supplier Solution they require. The Supplier shall retain an audit record of accesses.

11 Audit and Monitoring

11.1 The Supplier shall collect audit records which relate to security events in the systems or that would support the analysis of potential and actual compromises. In order to facilitate effective monitoring and forensic readiness such Supplier audit records should (as a minimum) include:

11.2 Logs to facilitate the identification of the specific asset which makes every outbound request external to the IT Environment (to the extent that the IT Environment is within the control of the Supplier). To the extent the design of the Detailed Solutions and Services allows such logs shall include those from DHCP servers, HTTP/HTTPS proxy servers, firewalls and routers.

11.3 Security events generated in the IT Environment (to the extent that the IT Environment is within the control of the Supplier) and shall include: privileged account logon and logoff events, the start and termination of remote access sessions, security alerts from desktops and server operating systems and security alerts from third party security software.

11.4 The Supplier and the Authority shall work together to establish any additional audit and monitoring requirements for the IT Environment.

11.5 The Supplier shall retain audit records collected in compliance with Paragraph 11 for a period of at least 6 months.

Annex 2 – Security Management Plan

The Security Management Plan shall be the document appended on the Initialled CD-ROM – Reference: 'CD - DWP SSA Schedule 2.4 Annex 2' attached to this Schedule.

The Parties acknowledge and agree that the Security Management Plan in the Initialled CD ROM – Reference: 'CD - DWP SSA Schedule 2.4 Annex 2' is correct and contractually binding and forms part of the Agreement in accordance with its terms and conditions.

Signed for and on behalf of **The Secretary of State for Work and Pensions**

…….

Date:……

Signed for and on behalf of **G4S Secure Solutions (UK) Limited**

…….

Date:……