SCHEDULE 18

INFORMATION ASSURANCE

1. INFORMATION ASSURANCE

The Contractor shall obtain and maintain an Information Security Management System (**ISMS**) in accordance with the following standards and policies set out in this Schedule 18 during the Contract Period.

1.1 ISO 27001

(a) The Contractor shall obtain by no later than the date that is 24 months after the Amendment Date and maintain during the Contract Period UKAS certification for its ISMS against ISO 27001:2013, the scope of which must include all Information Assets and any systems used to process the information relevant to the provision of the Services, the Contractor ICT and the Project Data.

(b) The Contractor shall provide the Authority, upon request, with any or all ISMS documentation as defined in ISO 27001.

(c) The Contractor shall appoint a senior representative with appropriate experience in security management who shall sit on the board of the Contractor, shall be responsible for the Contractor's ISMS and who shall be responsible for the compliance by the Contractor and the Contractor Personnel of the ISMS all in accordance with the management responsibilities as defined in ISO 27001.

(d) The Contractor shall throughout the Contract Period ensure that all Contractor Personnel and other staff and volunteers with access to Information Assets will be vetted as appropriate in relation to the level of data access required by that person pursuant PSI 07/2014 Security Vetting.

(e) The Contactor shall ensure that all Contractor Personnel who use the Authority ICT actively confirm annually their acceptance of the Authority's acceptable use policy, as amended from time to time by the Authority (a copy of which is set out on the Authority Website).

(f) The Contractor shall, in the event of non-compliance with this Schedule 18 or any other failure to comply with information security requirements under this Agreement including those set out in Schedule 19 (ICT) (a **Security Failure**):

(i) provide to the Authority for its review and approval, a plan which specifies how the Contractor proposes to redress each Security Failure (as the case may be) (a **Security Improvement Plan**). If the Authority objects to any part of the Security Improvement Plan, the matter shall be resolved in accordance with the Escalation Process; and

(ii) comply with the terms of the Security Improvement Plan and implement any changes as may be necessary to ensure compliance with this Schedule 18 or any other security requirements, as applicable.

The Authority acknowledges that the timetable for ensuring compliance in accordance with this paragraph 1.1(f) shall be set out by the Contractor in the Security Improvement Plan and

the Authority shall not require the Contractor to be in full compliance with ISO 27001 prior to the date that is 24 months from the Amendment Date.

1.2 **Security Policy Framework**

(a) The Contractor shall comply with, and shall procure that each Subcontractor complies with, the Security Policy Framework to effectively, collectively and proportionately manage and report on all security risks in the provision of the Services.

(b) The Contractor shall comply with the Mandatory Probation Instruction PI 03/2009 (Information Assurance).

2. INFORMATION SECURITY INCIDENT MANAGEMENT PROCEDURE

2.1 The Contractor shall implement a procedure for reporting, recording and managing information security incidents.

2.2 The Contractor shall report to the Authority in writing all Applicable Person information incidents and other high impact information incidents as identified in the Mandatory Probation Instruction PI 10/2012, promptly after the incident has been identified.

3. ANNUAL RETURN FOR SECURITY RISK MANAGEMENT OVERVIEW

The Contractor shall report in writing on an annual basis to the Authority the Contractor's experience in relation to implementing and managing the Security Policy Framework and managing Information Risk Management (as defined in ISO 27001), and shall identify any area in which it is not compliant with its obligations under this Schedule 18.

4. RECORD MANAGEMENT AND RETENTION

4.1 The Contractor shall implement an Information Record Management (IRM) Framework, which shall include the following:

(a) organisational arrangements;

(b) policy and procedures;

(c) record keeping;

(d) record systems;

(e) storage and maintenance of records;

(f) security access controls;

(g) disposal and preservation of records;

(h) partnering, outsourcing and shared services;

(i) monitoring and reporting mechanisms; and

(j) ensuring the segregation of records where the Contractor is co-locating with the Authority subject to the terms of a Lease and Licence Agreement.

4.2 The scope of the IRM Framework shall include full and accurate hard copy and/or electronic records for all of the Services.

5. DIGITAL CONTINUITY

The Contractor shall ensure that, for the Contract Period and all other applicable retention periods in this Agreement, each Information Asset is held in an appropriate format that is capable of being updated from time to time, to enable the Information Asset to be retrieved, accessed, used and transferred to the Authority in accordance with the information handling procedures set out in the Mandatory Probation Instruction PI 03/2009 (Information Assurance).

6. PRIVACY IMPACT ASSESEMENT (PIA)

6.1 The Contractor shall, as requested by the Authority, provide reasonable assistance to the Authority in performing a PIA in accordance with the guidance issued by the UK Information Commissioners Office.

6.2 Following completion of a PIA by the Authority, the Contractor shall provide to the Authority for approval a plan setting out the actions that the Contractor shall take to mitigate against all privacy risks identified during the Privacy Impact Assessment as being applicable to the Contractor (**Privacy Risk Treatment Plan**). If the Authority objects to any part of the Privacy Risk Treatment Plan, the matter shall be resolved in accordance with the Escalation Process. Following the approval by the Authority of the Privacy Risk Treatment Plan, the Contractor shall implement the Privacy Risk Treatment Plan. The costs of implementing the Privacy Risk Treatment Plan shall be met by the Contractor.