SCHEDULE X: INFORMATION ASSURANCE

1. INFORMATION ASSURANCE

In addition to the provisions of this Schedule, the Provider shall comply with the Information Assurance requirements in Schedule U (Information Security) of this Contract.

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

The Provider shall comply with the Mandatory Agency Instruction AI 18/2014 (Information Assurance).

ISO 27001

1.1 The Provider shall:

1.1.1 obtain by no later than the date that is 18 months after the Service Commencement Date and maintain during the Contract UKAS certification for its ISMS against ISO 27001:2013, the scope of which must include all Authority Data, Information Assets, any other data or information relevant to the provision of the Services and any systems on which this is processed and/or stored including the Provider's System;

1.1.2 provide the Authority, upon request, any or all ISMS documentation as defined in ISO 27001;

1.1.3 appoint a senior representative or representatives with appropriate experience in security management and information assurance, shall be responsible for the Provider's ISMS and who shall be responsible for the compliance by the Provider and any of its Sub-contractors with the ISMS in accordance with the management responsibilities as defined in ISO 27001;

1.1.4 throughout the Contract ensure that all Provider's Personnel with access to Authority Data, Information Assets and any other data or information relevant to the provision of the Services will be vetted as appropriate in relation to the level of data and information access required by that person pursuant PSI 07/2014 Security Vetting;

1.1.5 ensure that all Provider's Personnel who use the Authority System actively confirm annually their acceptance of the Authority's acceptable use policy, as amended from time to time by the Authority.

1.1.6 in the event of a Security Failure:

1.1.6.1 provide to the Authority for its review and Approval, a Security Improvement Plan. If the Authority objects to any part of the Security

Improvement Plan, the matter shall be resolved in accordance with clause 67 (Dispute Resolution) of the Contract; and

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

1.2 The Authority acknowledges that the timetable for ensuring compliance in accordance with this Paragraph 1.1(f) shall be set out by the Provider in the Security Improvement Plan and the Authority shall not require the Provider to be in full compliance with ISO 27001 prior to the date that is 18 months from the Service Commencement Date.

Security Policy Framework

1.3 The Provider shall comply with, and shall procure that all Provider's Personnel comply with the Security Policy Framework to effectively, collectively and proportionately manage and report on all security risks in the provision of the Services.

2. INFORMATION SECURITY INCIDENT MANAGEMENT PROCEDURE

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

2.2 The Provider shall report to the Authority in writing all information incidents and other high impact information incidents as identified in the Mandatory Prison Service Instruction PSI 24/2014 (Information Assurance), promptly after the incident has been identified.

3. ANNUAL RETURN FOR SECURITY RISK MANAGEMENT OVERVIEW

The Provider shall report in writing on an annual basis to the Authority the Provider'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.

4. RECORD MANAGEMENT AND RETENTION

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

4.1.1 organisational arrangements;

4.1.2 policy and procedures;

4.1.3 record keeping;

4.1.4 record systems;

4.1.5 storage and maintenance of records;

4.1.6 security access controls;

4.1.7 disposal and preservation of records;

4.1.8 partnering, outsourcing and shared services;

4.1.9 monitoring and reporting mechanisms; and

4.1.10 ensuring the segregation of records where the Provider is co-locating with the Authority.

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

5. DIGITAL CONTINUITY

The Provider shall ensure that, for the duration of this Contract and all other applicable retention periods in this Contract, 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 Prison Service Instruction PSI 24/2014 (Information Assurance).

6. PRIVACY IMPACT ASSESEMENT (PIA)

6.1 The Provider 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 Provider shall provide to the Authority for Approval a 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 Dispute Resolution procedure at clause 67 of this Contract. Following the Approval by the Authority of the Privacy Risk Treatment Plan, the Provider shall implement the Privacy Risk Treatment Plan. The costs of implementing the Privacy Risk Treatment Plan shall be met by the Provider.