CONTRACT REFERENCE NUMBER: 17/01/54

SERVICES CONTRACT

-between-

(1) THE REGISTRAR GENERAL OF BIRTHS, DEATHS AND MARRIAGES FOR SCOTLAND (THE "AUTHORITY")

-and-

(2) CACI LIMITED (THE "SERVICE PROVIDER")

-relating to the supply of-

SERVICES FOR

THE PROVISION OF AN ONLINE COLLECTION INSTRUMENT FOR SCOTLAND'S CENSUS 2021

SCHEDULE 12

SECURITY MANAGEMENT

This and the six (6) following pages comprise Schedule 12 referred to in the foregoing Services Contract between the Registrar General of Births Deaths and Marriages for Scotland and CACI Limited

1. **SECURITY ARRANGEMENTS**

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

1.2. The Service Provider shall ensure the up-to-date maintenance of a suitable 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.

1.3 The Service Provider shall ensure their Key Individuals in Schedule 4 *(Management Arrangements, Implementation Plan, Key Individuals and Approved Subcontractors)* responsible for Security Management regularly attend the Authority's Security Working Groups

2. SECURITY PLAN

2.1 Within 20 Working Days after the Commencement Date, the Service Provider shall prepare and submit to the Authority for approval in accordance with Paragraph 2.3 a fully developed, complete and up-to-date Security Plan which shall comply with the requirements of Paragraph 2.2.

2.2 The Security Plan shall:

(a) meet the relevant standards in ISO/IEC 27001:2013 in accordance with Paragraph 5; and

(b) at all times provide a level of security which:

(i) is in accordance with Law and this Contract;

(ii) as a minimum demonstrates Good Commercial Practice;

(iv) addresses issues of incompatibility with the Service Provider's own organisational security policies;

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

(vi) complies with the security requirements as set out in Schedule 2 The Services *(Specification and Service Provider Solution))*;

(vii) complies with the Authority's IT policies; and

(viii) is in accordance with the Security Policy Framework.

(c) document the security incident management processes and incident response plans applicable to the Services;

(d) 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 Service Provider 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;

(e) identify the necessary delegated organisational roles defined for those responsible for ensuring this Schedule is complied with by the Service Provider;

(f) detail the process for managing any security risks from Sub-contractors and third parties authorised by the Authority with access to the Services, processes associated with the delivery of the Services, the Authority Property, the sites used by the Service Provider to deliver the Services, the Service Provider's System, the Service Provider Solution, the Authority's System (to extent that it is under the control of the Service Provider) and any IT,

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

(g) 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 Property, the sites used by the Service Provider to deliver the Services, the Service Provider's System, the Service Provider Solution, the Authority's System (to the extent that it is under the control of the Service Provider) and any IT, information and data (including the Authority Confidential Information and the Data) to the extent used by the Authority or the Service Provider in connection with this Contract or in connection with any system that could directly or indirectly have an impact on that Information, data and/or the Services;

(h) set out the security measures to be implemented and maintained by the Service Provider 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.

(i) demonstrate that the Service Provider Solution has minimised the Authority and Service Provider 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);

(j) be structured in accordance with ISO/IEC 27001:2013, cross referencing if necessary to other Schedules which cover specific areas included within those standards;

(k) be written in plain English in language which is readily comprehensible to the staff of the Service Provider 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; and

(l) be in accordance with the Security Policy Framework.

2.3 The Service Provider shall update the Security Plan in accordance with any comments from the Service Provider, and shall review and revise the Security Plan regularly (or as per such other time period as agreed between the Parties) all in accordance with Paragraph 3 (such updates shall incorporate any comments received from the Authority).

2.4 The Service Provider shall deliver all Services in accordance with the Security Plan.

3. AMENDMENT AND REVISION OF THE SECURITY PLAN

3.1 The Security Plan shall be fully reviewed and updated by the Service Provider regularly to reflect:

(a) emerging changes in Good Commercial Practice;

(b) any change or proposed change to the Service Provider's Solution, the Services and/or associated processes;

(c) any new perceived or changed security threats; and

(d) any reasonable change in requirement requested by the Authority.

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

(a) suggested improvements to the effectiveness of the Security Plan;

(b) updates to the risk assessments;

(c) proposed modifications to respond to events that may impact on the Security Plan including the security incident management process, incident response plans and general procedures and controls that affect information security; and

(d) suggested improvements in measuring the effectiveness of controls.

3.3 Subject to Paragraph 3.4, any change which the Service Provider proposes to make to the Security Plan (as a result of a review carried out pursuant to Paragraph 3.1, an Authority request, a change to Schedule 2 *The Services (Specification and Service Provider Solution)* or otherwise) shall be subject to the Change Control Procedure and shall not be implemented until approved in writing by the Authority.

3.4 The Authority may, where it is reasonable to do so, approve and require changes or amendments to the Security 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 Contract.

4. SECURITY TESTING

4.1 Security Tests shall be designed and implemented by the Authority who will coordinate with the Service Provider 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 Service Provider. Subject to compliance by the Service Provider with the foregoing requirements, if any Security Tests adversely affect the Service Provider's ability to deliver the Services so as to meet the Service Levels, the Service Provider shall be granted relief against any resultant under-performance for the period of the Security Tests.

4.2 Where any Security Test carried out reveals any actual or potential Breach of Security or weaknesses (including un-patched vulnerabilities, poor configuration and/or incorrect system management), the Service Provider shall promptly notify the Authority of any changes to the Security Plan (and the implementation thereof) which the Service Provider proposes to make in order to correct such failure or weakness. Subject to the Authority's prior written approval, the Service Provider shall implement such changes to the Security 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 Security Plan is to address a non-compliance with the security requirements (as set out in Schedule 2 *The Services (Specification and Service Provider Solution))* or the requirements of this Schedule, the change to the Security Plan shall be at no cost to the Authority.

4.3 If any repeat Security Test carried out pursuant to Paragraph 4.2 reveals an actual or potential Breach of Security exploiting the same root cause failure, such circumstance shall be deemed to constitute a Delay for the purposes of Clause 26.3 (*Rectification Plan*) and be dealt with accordingly in terms of Clause 26.3 (*Rectification Plan*).

5. SECURITY PLAN COMPLIANCE

5.1 The Authority shall be entitled to carry out such security audits as it may reasonably deem necessary in order to ensure that the Security Plan maintains compliance with the principles and practices of ISO 27001:2013, and the specific security requirements set out in Schedule 2 *The Services (Specification and Service Provider Solution)*).

5.2 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 27001:2013, the specific security requirements set out in Schedule 2 *The Services (Specification and Service Provider Solution)*is not being achieved by the Service Provider, then the Authority shall notify the Service Provider of the same and give the Service Provider 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 Service Provider 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.

5.3 If, as a result of any such independent audit as described in paragraph 5.2 the Service Provider is found to be non-compliant with the principles and practices of ISO/IEC 27001:2013, the specific security requirements set out in Schedule 2 The Services *(Specification and Service Provider Solution)* then the Service Provider shall, at its own expense, immediately 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.

6. BREACH OF SECURITY

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

6.2 Without prejudice to the security incident management process, upon becoming aware of any of the circumstances referred to in paragraph 6.1, the Service Provider shall:

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

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

(ii) remedy such Breach of Security to the extent possible and protect the integrity of the Authority's System, the Service Provider's System and the Service Provider Solution to the extent within its control against any such Breach of Security or attempted Breach of Security;

(iii) 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 Service Provider, if the mitigation adversely affects the Service Provider's ability to deliver the Services so as to meet the Service Levels, the Service Provider shall be granted relief against any resultant under-performance for such period as the Authority, acting reasonably, may specify by written notice to the Service Provider;

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

(v) supply any requested data to the Authority within 2 Working Days of the Authority's request and without charge (where such requests are reasonably related to a possible incident or compromise); and

(b) as soon as reasonably practicable provide to the Authority full details (using the reporting mechanism defined by the Security Plan) of the Breach of Security or attempted Breach of Security, including a root cause analysis where required by the Authority.

6.3 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 Security Plan with the security requirements (as set out in Schedule 2 The Services *(Specification and Service Provider Solution))* or the requirements of this Schedule, then any required change to the Security Plan shall be at no cost to the Authority.

7. VULNERABILITIES AND CORRECTIVE ACTION

7.1 The Authority and the Service Provider acknowledge that from time to time vulnerabilities in the Authority's System, the Service Provider's System and the Service Provider Solution will be

discovered which unless mitigated will present an unacceptable risk to the Authority's information, including Data.

7.2 The severity of threat vulnerabilities for the Services shall be categorised by using an appropriate vulnerability scoring systems including:

(a) 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/or

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

7.3 The Service Provider shall ensure the application of security patches to vulnerabilities in a timely and prioritised manner.

7.4 The Service Provider shall ensure all Service Provider COTS Software and Third Party COTS Software are 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.

7.5 The Service Provider shall:

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

(b) ensure that the Authority's System, the Service Provider's System and the Service Provider Solution (to the extent that the Authority's System, the Service Provider's System and the Service Provider Solution is within the control of the Service Provider) is monitored to facilitate the detection of anomalous behaviour that would be indicative of system compromise;

(c) ensure it is knowledgeable about the latest trends in threat, vulnerability and exploitation that are relevant to the Authority's System, the Service Provider's System and the Service Provider Solution by actively monitoring the threat landscape during the Term;

(d) pro-actively scan the Authority's System, the Service Provider's System and the Service Provider Solution (to the extent that the Authority's System, the Service Provider's System and the Service Provider Solution is within the control of the Service Provider) for vulnerable components and address discovered vulnerabilities through the processes described in the Security Plan as developed under paragraph 2.2(e);

(e) 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 Authority's System, the Service Provider's System and the Service Provider Solution (to the extent that the Authority's System, the Service Provider's System and the Service Provider Solution is within the control of the Service Provider) 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;

(f) propose interim mitigation measures to vulnerabilities in the Authority's System, the Service Provider's System and the Service Provider Solution known to be exploitable where a security patch is not immediately available;

(g) 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 Service Provider Solution and the Authority's System, the Service Provider's System and the Service Provider Solution); 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 Authority's System, the Service Provider's System and the Service Provider Solution and provide initial indications of possible mitigations.

7.6 If the Service Provider is unlikely to be able to mitigate the vulnerability within a timely manner under paragraph 7, the Service Provider shall immediately notify the Authority.

ANNEX 1: SECURITY PLAN

[To be inserted]

Signature ……. Signature ……..