Home Office

AUTHORITY: The Secretary of State for the Home Department

Schedule 2.2 – Security

Secure English Language Testing Services

Trinity College London

DOCUMENT LIST

Volume	Title
	Concession Agreement
Schedules to Concession Agreement	SCHEDULE 1 Definitions
	SCHEDULE 2 Concession Requirement 2.1 Authority's Requirements **2.2 Security** 2.3 Service Levels, Performance and Liquidated Damages
	SCHEDULE 3 Concessionaire's Solution
	SCHEDULE 4 Concessionaire Matters 4.1 Sub-Contractors 4.2 Commercially Sensitive Information
	SCHEDULE 5 IPR 5.1 Intellectual Property Rights
	SCHEDULE 6 Mobilisation 6.1 Mobilisation and Permit to Operate
	SCHEDULE 7 Financial Matters 7.1 Fees 7.2 Form of Guarantee
	SCHEDULE 8 Governance & Process 8.1 Governance and Contract Management 8.2 Change Control Procedure 8.3 Dispute Resolution Procedure 8.4 Audits, Records and Assurance 8.5 BCDR Plan 8.6 Exit Management 8.7 Management Information
	SCHEDULE 9 Personnel Matters 9.1 Personnel Transfer 9.2 Personnel and Key Representatives 9.3 Personnel Clearance Procedure

CONTENTS

1. INTRODUCTION

1.1 This Schedule describes the Authority's security requirements that the Concessionaire is required to meet or exceed during the Term.

1.2 If and to the extent of any conflict or inconsistency between Annex 2.2-1 and/or Annex 2.2-2 and Paragraphs 1 to 11 of this Schedule 2.2 (Security), Paragraphs 1 to 11 shall prevail.

2. SECURITY POLICIES

2.1 The Concessionaire shall deliver the Services to the Authority in accordance with the **HMG Security Policy Framework** and in accordance with Annex 2.2-1 **(**The Authority's Security Policy).

2.2 The Authority continues to keep the Authority Security Policy under review. Changes shall be made to the Authority Security Policy from time to time, in response to appropriate changes in the HMG Security Policy Framework, and as required for other reasons.

2.3 The Concessionaire shall have an independent assurance statement completed of its compliance with the HMG Security Policy Framework and with the Authority's Security Policy as set out in Annex 2.2-1 to this Schedule 2.2 (Security).

2.4 Changes to the Concessionaire's Solution and the Authority's Requirements which are necessary to meet changes occurring after the PTO Commencement Date to the Authority's Security Policy and/or the HM Government's Security Policy shall be agreed through Schedule 8.2 (Change Control Procedure).

2.5 Any changes to the Concessionaire's Solution required, either as a result of changes to HM Government's Security Policy Framework or to reflect Good Industry Practice shall be agreed as a non-chargeable Change.

3. SECURITY PLAN

3.1 The Concessionaire shall develop and agree with the Authority, a Security Plan which shall form Annex 2.2-2 to this Schedule 2.2 (Security). The Security Plan applies, in particular, to the security of the Authority's tests, data and other information.

3.2 The Concessionaire shall comply, in operating Test Centres, with the agreed Security Plan which:

3.2.1 is consistent with and complies with the relevant aspects of the Authority's Security Policy and Security Standards, as set out in Annex 2.2-1;

3.2.2 conforms to appropriate UK Government security policies, standards and guidance and specifically HMG Security Policy Framework issued by Cabinet Office; CESG information assurance standards and guidance and successor documents;

3.3.3 complies with ISO/IEC 27001; and

3.3.4 meets the other security requirements set out in this Schedule 2.2 (Security) and any other part of this Concession Agreement.

For the avoidance of doubt, compliance with HMG Security Policy Framework (SPF) shall take precedence, in the event of any conflict between any of the requirements listed above.

3.3 The Concessionaire acknowledges that the key aims of the Security Plan are to provide:

3.3.1 appropriate protection (as specified in paragraph 2.1 above) in relation to the protection of people, premises, property, tests and other information (in all its forms) against attack, theft, disclosure, unauthorised access, corruption or non-availability, whether by deliberate or accidental means; and

for co-operation with the Authority in any investigation that is necessary to safeguard the Authority's data and assets.

3.4 The Security Plan shall be supported by appropriate organisational, security and technical security standards.

4. SUB-CONTRACTORS

4.1 Where sub-contracting is permitted, the Concessionaire shall ensure that Concessionaire Sub-contractors comply with the Security Plan in the same way as the Concessionaire is required to comply with the Security Plan. Each Concessionaire Sub-contract shall include such aspects of this Schedule as are appropriate to the Authority's Requirements to be fulfilled by that Concessionaire Sub-contractor at the date of such contract.

4.2 Without prejudice to paragraph 11 below, the Concessionaire shall carry out Operational audits of the Concessionaire Sub-contractors and the Test Centres used by Concessionaire Sub-contractors in the fulfilment of the Authority's Requirements in accordance with Schedule 8.4 (Audits, Records and Assurance) and at intervals agreed with the Authority and shall make audit reports available to the Authority. The Concessionaire shall use Commercially Reasonable Efforts to ensure that each Concessionaire Sub-contract imposes flow down provisions as set out in Schedule

4.1 (Sub-contractors) to enable the Authority to conduct audits of the Concessionaire Sub-contractor as outlined in Schedule 8.4 (Audits, Records and Assurance).

4.3 Where the Concessionaire is permitted to (as per Schedule 4.1 ((Sub-contractors)) and wishes to sub-contract the provision of services to a potential Concessionaire Sub-contractor, the Concessionaire shall first conduct a security survey on that potential Concessionaire Sub-contractor's existing process, procedures, information systems and Test Centres as part of the assessment of the potential Concessionaire Sub-contractor's suitability to act as a Concessionaire Sub-contractor, in order to identify gaps in security. The Concessionaire shall flow-down its security obligations in any resulting Concessionaire Sub-contract with the potential Concessionaire Sub-contractor and during Mobilisation, the Mobilisation Lead, shall work with the Concessionaire Sub-contractor to ensure that relevant security gaps are rectified.

5. MANAGING SECURITY

5.1 The Concessionaire shall nominate an individual to be accountable for the management of security and for assurance of the Authority's data, in relation to the Concession Agreement (the "Concessionaire Security Lead"). The approval is to be in accordance with Schedule 9.3 (Personnel Clearance Procedure).

5.2 The responsibilities of the Concessionaire Security Lead shall include the following:

5.2.1 representing the Concessionaire at all meetings that address security concerns, events and issues, except where the Authority expressly requires otherwise;

5.2.2 ensuring that security is integrated into the Concessionaire's and the Concessionaire's Sub-contractors' day-to-day working with respect to the Authority's Requirements;

5.2.3 receiving service updates on a Monthly basis relating to security activities from each of the Concessionaire nominated individuals responsible for each component of the Authority's Requirements. Such nominated individuals shall further report Security Incidents promptly to the Concessionaire Security Manager, who shall be responsible for reporting all such incidents using the Concessionaire's own protocols on escalating information internally, and/or to the Authority and/or to Ofqual as deemed appropriate to the nature of the incident (considering scale, potential impact and recurrence)

5.2.4 attending Contract Management meetings, when convened by the Authority; and

5.2.5 giving assurance to the Authority via the Monthly report that the Concessionaire and its Personnel in operating the Test Centres, are adhering to the requirements of this Schedule 2.2 (Security).

5.3 The Concessionaire shall deliver assurance to the Authority, within a reasonable time of a request by the Authority for such assurance, that the Concessionaire's Solution complies with UK Government security policies, standards and guidance and, specifically, HMG Security Policy Framework and the Authority's Security Policy, or that an appropriate risk management decision (agreed in writing by duly authorised representatives of the Authority) enables the Concessionaire's Solution to be delivered without complying with the Authority's Security Policy and the HMG Security Policy Framework.

5.4 The Authority may, at any time, convene a meeting to monitor the Concessionaire's management of security; discuss and resolve security issues and share information.

5.6 The Concessionaire shall provide to the Authority regular reports on the status of security within the scope of the Authority's Requirements, as specified in Schedule 8.7 (Management Information).

6. AUTHORISATION OF CONCESSIONAIRE PERSONNEL

6.1 All persons (including all personnel engaged by Concessionaire Sub-contractors) whom the Concessionaire proposes to carry out work or perform duties under the Concession Agreement and who shall be required, while carrying out some or all of that work or performing some or all of those duties, to:

6.1.1 enter secure areas in Concessionaire Test Centres;

6.2.2 access the Technical Infrastructure;

6.2.3 work with Authority Personnel for extended periods; and/or

6.2.4 have access to Authority Data;

must hold a particular kind of security clearance (as described in Schedule 9.3 (Personnel Clearance Procedure)).

7. PHYSICAL SECURITY

7.1 General

7.1.1 The Concessionaire shall have appropriate and adequate security measures to ensure the operational integrity of the Secure English Language Test Process.

7.1.2 During the Concession Agreement Term and in accordance with paragraph 2.1, the Concessionaire is responsible for and shall put in place appropriate security measures for the protection of:

i. Concessionaire Personnel, Candidates and/or any Authority Personnel attending the Test Centre;

ii. the integrity of the test and the results given to Candidates;

iii. the Test Centre, property and assets used to provide the Concessionaire's Solution, including any Assets, Materials or Software provided to the Concessionaire by the Authority; and

iv. information (in all its forms), against attack, theft, disclosure, unauthorised access, corruption or non-availability, as applicable, whether by deliberate or accidental means.

7.1.3 As part of the Concessionaire's Solution, the Concessionaire shall ensure that the location chosen for the Test Centre is safe and fit for purpose from a physical security perspective. The Concessionaire shall obtain the Authority's consent to the Test Centre in accordance with Schedule 6.1 (Mobilisation and Permit to Operate). The Authority reserves the right to seek expert advice from the Foreign and Commonwealth Office to inform its decision as to the location of a Test Centre.

7.1.4 The Concessionaire is responsible for putting in place appropriate security measures to protect the perimeter of the Test Centres.

7.1.5 The Concessionaire is responsible for providing appropriate protection (as specified in paragraph 2.1 above), in accordance with the Authority's Security Policy And Security Standards and in accordance with the Security Plan, for the health and safety of all Concessionaire Personnel, Authority Personnel, Test Candidates and any other persons located on or visiting Concessionaire Test Centres.

7.1.6 Access to public areas of Test Centres shall be restricted to Test Candidates and any companions thereof, who are required to support the Test Candidate, *e.g*. a companion may be required in the case of a disabled or infirm Test Candidate or when the Test Application is in respect of a minor. The Concessionaire shall restrict access to Concessionaire Test Centres and the Technical Infrastructure to Authorised Personnel only.

7.1.7 The Concessionaire shall provide appropriate protection (as specified paragraph 2.1 above) to ensure that any access to Concessionaire Test Centres and/or the Technical Infrastructure is strictly limited to such part of the

Concessionaire Test Centres or Technical Infrastructure as is required for the proper performance of the Concessionaire's obligations under this Concession Agreement.

7.1.8 The Concessionaire shall use appropriate protection (as specified in paragraph 2.1 above) to ensure that Test Candidates and other members of the public cannot access non-public areas of the Test Centres or the Technical Infrastructure.

7.2 Concessionaire's Security Plan for Test Centres

7.2.1 Annex 2.2-2 of this Schedule sets out the Concessionaire's Security Plan that the Concessionaire shall put in place for each Test Centre. The Parties acknowledge that such Security Plan shall apply from the relevant Commencement Date for each Test Centre. However, the Parties acknowledge that the Concessionaire's Security Plan in Annex 2.2-2 may need to change as a result of the security risk assessment described in paragraph 7.2.2 below, as agreed in accordance with Schedule 8.2 (Change Control Procedure).

7.2.2 At least one (1) month (where possible, in accordance with the Local Mobilisation Plan) prior to the relevant Commencement Date for each relevant Test Centre, the Concessionaire shall carry out a security risk assessment of the relevant Test Centre, taking into account its location, to confirm if the physical security standards and measures in Annex 2.2-2 are sufficient to meet the Concessionaire's security obligations under paragraph 7.1 above. Such security risk assessment may include a gap analysis or other processes to determine the Test Centre's physical security compliance with Annex 2.2-2.

7.2.3 It is acknowledged by the Parties that a Test Centre's security compliance with this Schedule 2.2 (Security) is one of the criteria for the Permit to Operate.

8. DATA SECURITY

8.1 The Concessionaire shall manage the risk of compromise to the confidentiality, integrity and availability of data and information by implementing information assurance processes and solutions that adhere to HMG Information Assurance Standards.

8.2 The Concessionaire shall provide appropriate protection to ensure that the Concessionaire Personnel and the Concessionaire Sub-contractors and their personnel do not attempt to access, or allow access to:

8.2.1 any data, files or programs used in the provision of the Services within the information systems environment;

8.2.2 the Authority's Materials; or

8.2.3 the Authority's Data, including test results

to which they do not need access in order to provide the Services, or which they are prohibited from accessing under the Concession Agreement or by Law.

8.3 The Concessionaire's Security Plan and policies must comply as a minimum with the requirements of the Data Protection Legislation as well as any relevant local data protection legislation. The Concessionaire, working together with the Authority, shall protect Personal Data relating to the Concession in accordance with the Data Protection Act.

8.4 The Concessionaire's Security Plan shall include how risks associated with loss of data confidentiality, integrity or availability of Candidate Data will be mitigated appropriately whilst such data is in the control of the Concessionaire, which shall include whilst the Candidate Data is in transit between the Test Centres.

8.5 The Concessionaire will notify the Authority immediately of any data loss whilst under its, or its Concessionaire Sub-contractors', control.

8.6 The Concessionaire's Security Plan shall also include a description of how:

8.6.1 risks associated with the obtaining of unauthorised access by anyone who does not require such access in order to carry out their obligations under this Concession Agreement will be mitigated;

8.6.2 the Concessionaire will prevent unauthorised personnel from gaining access to Authority Data; and

8.6.3 the Concessionaire will maintain systems security measures to guard against the unauthorised, alteration or destruction of Authority Material and Authority Data.

8.7 The Concessionaire shall assist the Authority, and/or other bodies sanctioned by the Authority, in the investigation of any incident of unauthorised or attempted disclosure or tampering with the Authority's information.

8.8 The Concessionaire Personnel and the Concessionaire Sub-contractors and their personnel shall not:

8.8.1 collect, stop, process or otherwise make use of Authority Data for any purpose other than that which is directly in relation to the supply of the Services;

8.8.2 purport to sell, let for hire, assign rights in or otherwise dispose of any of Authority Data;

8.8.3 make any of Authority Data available to any third party, other than to the extent necessary to enable that person to perform its part of the Services, and then only to that extent; or

8.9.4 commercially exploit Authority Data.

8.9 Without prejudice to the other rights of the Authority under this Concession Agreement, if in the provision of the Services any Authority Data is lost through the fault or negligence of the Concessionaire Personnel, or the Concessionaire Sub-contractors or their personnel, or any breach by the Concessionaire of the terms of this Concession Agreement, the Concessionaire shall regenerate such Authority Data to the most current back-up copy as required by the Concession Agreement without additional expense to the Authority and, in doing so, shall use its Commercially Reasonable Efforts to ensure that the timings for the provision of the Services are not materially affected.

8.10 The Concessionaire may from time to time be required to respond to additional requests from the Authority for assurance regarding the handling of information, to enable the Authority to assess the maturity of the Concessionaire's information handling policies and procedures.

8.11 The Concessionaire will continually review the known and possible risks and will ensure that the relevant risks are taken into consideration when planning, selecting, designing and modifying its Test Centres for delivering the Services.

9. SECURITY INCIDENTS

9.1 The Concessionaire's Security Plan shall include a description of how all violations of the Security Policy will be reported internally, to the Authority and to Ofqual where appropriate.

9.2 In addition to the Concessionaire's reporting obligation agreed under paragraph 9.1 above, if a Security Incident occurs, the Concessionaire shall carry out an immediate investigation into the incident and initiate corrective actions to minimise the possibility of re-occurrence. The Concessionaire shall also prepare and retain documentation of the investigation of the violation and provide a copy to the Authority. Within 1 (one) month of notifying the Authority via the Compromised Testing notification it will provide a full report.

9.3 The Authority shall have the right to investigate any or all Security Incidents, security concerns or unresolved security issues or refer incidents to the Police and others, as required. .

10. INSPECTION

10.1 The Authority shall have the right to inspect any and all security aspects of the Concessionaire's operations in accordance with Schedule 8.4 (Audits, Records and Assurance) in order to verify compliance with the Security Policy and the Security Standards and this Schedule, including attending the Test Centres, to inspect the physical security and procedural security standards and measures in place.

11. SPECIFIC SECURITY REQUIREMENTS

Specific Security Requirements during Mobilisation

11.1 In addition to the other provisions of this Schedule 2.2 (Security), for the purposes of demonstrating its compliance with the Authority's Security Policy and Security Standards in respect of Mobilisation, the provisions below in paragraph 11.2 shall apply to all Test Centres. For the avoidance of doubt, this process and the activities outlined in Paragraph 11.2 and/or the security controls set out in Annex 2.2-2 do not represent the Authority's sign-off or acceptance that the security measures put in place by the Concessionaire comply with the provisions of this Schedule 2.2 (Security); during the Concession Agreement Term, it shall remain the Concessionaire's responsibility to ensure it remain in compliance with this Schedule 2.2 (Security).

11.2 Control of Biometric equipment

11.2.1 The Concessionaire is responsible for ensuring that Business Continuity Plans covering any Biometric Equipment provided by or purchased from the Authority have been approved and signed-off by the Authority's management team prior to the Commencement Date for go live in each Test Centre.

11.2.2 The Concessionaire's Security Plan shall include a description of how risks associated with storage and transportation of Biometric Equipment will be mitigated appropriately. Particular attention should be made to risks associated with temporary storage and mobile use.

11.2.3 The Concessionaire shall keep an audit trail detailing when, where and by whom the Biometric Equipment is used. This log will be made available to the Authority during inspections of the operation of the Test Centres.

11.3 Loss of Biometric Equipment

11.3.1 In the event of loss or theft of the Biometric Equipment, the Concessionaire shall immediately report the Incident to the Concessionaire Security Lead and the Authority Concession Manager.

11.3.2 In the event of loss or theft of the Biometric Equipment, the Authority shall be entitled to carry out an investigation into the relevant incident and initiate corrective actions to minimise loss, damage and/or re-occurrence of the incident, including the right to cancel any Pop-Up Test Centre in that location, premises, Country and/or Region if the Authority determines, at the Authority's sole discretion, that such cancellation is necessary.

11.3.4 In the event of any loss or damage by the Concessionaire to the Biometric Equipment, the Concessionaire shall be responsible for the cost of repair or replacement of the Biometric Equipment at a charge to be agreed with the Authority.

11.4 Loss of Biometric Data

11.4.1 If the Concessionaire believes that Biometric Data has been or will be compromised, damaged or lost, or is aware of any unauthorised access, corruption or impostors, the Concessionaire shall immediately provide a detailed information report to the Concessionaire Security Lead and the Authority's Concession Manager.

11.4.2 In the event of an incident of the type described in Paragraph 11.4.1 above, the Authority is entitled to carry out an investigation into the incident and initiate corrective actions to minimise loss, damage and/or re-occurrence of the incident, including the right to cancel any Pop-Up Test Centres in that location/premises, Country and/or Region if the Authority determines, at the Authority's sole discretion, that such cancellation is necessary.

Pop-Up Test Centres

11.5 General

11.5.1 This Paragraph 11.5 to Paragraph 11.10 (inclusive) of Schedule 2.2 (Security) describes the additional security requirements that the Concessionaire is required to meet or exceed during the Concession Agreement Term in the delivery of Pop-Up Test Centres.

11.5.2 The security requirements of Annex 2.2-1 of Schedule 2.2 (Security) shall apply equally to Pop-Up Test Centres, except where otherwise agreed to by the Authority. Annex 2.2-2 (Concessionaire Security Plan), incorporates the Concessionaire's Solution in relation to the security requirements set out in Paragraphs 11.5 to 11.11 of this Schedule 2.2 (Security). If and to the extent there is any conflict or inconsistency between Annex 2.2-2 and Paragraphs 11.5 to 11.12 of Schedule 2.2 (Security), shall prevail.

11.5.3 Annex 2.2-1 of this Schedule 2.2 (Security) describes the security requirements for a Test Centre. The Concessionaire Security Plan for a Pop-Up Test Centre shall aim to fully implement the security requirements of Annex 2.2-1. However, the Authority recognises that, due to the variation in locations used for a Pop-Up Test Centre, the full requirements of Annex 2.2-1 may not always be appropriate. Where this is the case, the Concessionaire shall propose to the Authority a Security Plan for each relevant Pop-Up Test Centre, based on the Risk Assessment process described in paragraph 11.5.2 above. The Authority shall consider the individual circumstances of the Pop-Up Test Centre when deciding whether the Security Plan proposed by the Concessionaire is appropriate. The Authority reserves the right to require the Concessionaire to implement in full the requirements of Annex 2.2-1 for any individual Pop-Up Test Centre.

11.7 Security at Pop-Up Test Centres

11.7.1 The Concessionaire shall ensure that appropriate security measures are in place that will allow for protection of any Biometric Equipment, Concessionaire Personnel, and Test Candidates at each Pop-Up Test Centre.

11.10 Anti Fraud and Corruption

11.10.1 All Concessionaire providing services to the Authority are required to put in place appropriate counter fraud and security management arrangements prior to the Commencement Date of the contract. Within one (1) month of the Commencement Date the Concessionaire shall complete a risk assessment of its counter fraud and security management arrangements. The risk assessment shall be provided to the Authority for consideration by a nominated counter-fraud specialist.

11.10.2 Any allegations of corrupt activity received by the Concessionaire in relation to the service delivered for the Authority must be copied immediately to the Authority's Corporate Security, the Authority Security Lead and Authority Concession Manager. The Concessionaire must appoint a single point of contact in relation to investigation matters.

11.10.3 Independent systems must be in place to report whistle blowing allegations. All Concessionaire Personnel should be provided with the details of the direct telephone number of the relevant team of counter-fraud specialists for the Authority.

11.10.4 In accordance with Schedule 8.4 (Audits, Records and Assurance) Concessionaire Personnel are required to cooperate fully with any investigation into fraud or corruption. Fraud investigators appointed by the

Authority must be given full and immediate access to all systems and records held by the Concessionaire and to their staff. The Authority shall at any time during the provision of the Services, be able to give the Concessionaire immediate notice requiring the removal from the Concessionaire's premises of any equipment, documentation or other evidence which, in the reasonable opinion of the Authority's Representative is required as evidence of part of an investigation.

11.10.5 The Concessionaire shall ensure that the Authority is allowed access, to all of the Concessionaire Test Centres in accordance with paragraph 6.2 of Schedule 8.4 (Audits, Records and Assurance) to conduct on site inspections for the purpose of fraud prevention, security policy and security requirements and compliance monitoring.

11.10.6 The Concessionaire shall employ appropriate counter fraud and anti-corruption measures to ensure the prevention of fraudulent activity within the delivery of the Services. These measures shall include: role and duty separation for business processes within sensitive areas, additional vetting requirements for sensitive posts and audit and analysis tools for monitoring system access and user activity.

11.10.7 The Concessionaire shall ensure that its anti-collusion and anti-fraud measures address the particular issues associated with Pop-Up Test Centres.

11.11 Breach of Security

11.11.1 Either Party shall notify the other in accordance with the agreed security incident management process as documented in the Security Plan upon becoming aware of any Breach of Security or any potential Breach of Security.

11.11.2 The Concessionaire shall ensure that all security incidents are reported in line with Compromised Testing Notification process, and that suspected security weaknesses of which it is aware are dealt with promptly in accordance with the Security Plan and an action plan to stop reoccurrence is agreed with the Authority.

ANNEX 2.2-1 TO SCHEDULE 2.2 (SECURITY) - THE AUTHORITY'S SECURITY POLICY

The Concessionaire's Security Plan must conform to HMG Security Policy Framework located at:
http://www.cabinetoffice.gov.uk/resource-library/security-policy-framework

This Annex 2.2-1 sets out the Authority's requirements for physical security at Test Centres, in order to ensure appropriate protection of Test Candidates, Concessionaire Personnel, Biometric Equipment, and any Authority Data.

The concessionaire must ensure that Test Centre environments meet the business requirements listed below and are inline with the business requirements listed below:

- **Each Test Centre shall have:**
    - A secure Test room with invigilator(s) present at all times during the Test
    - A reception and waiting area separate from the test room. Candidates who have taken a Test shall not be able to wait with Candidates yet to be tested.
    - Separate Male/Female and disabled toilets
    - Fire detection equipment and alarms
    - Clearly marked fire exits
    - Clearly displayed fire evacuation procedures
    - Secure storage of Candidates' belongings separate from the Test room
    - Secure storage of Test Materials
    - Defined and documented processes for the secure movement and handling of Test Materials
    - Security arrangements in place, in particular where computer-based Tests are delivered, to prevent access to other computer based tools, including the internet.
    - Defined and documented controls on the presence of anyone other than Candidates/examiners/invigilators/interlocutors in the Test room.
    - A workstation for each Candidate, equipped with computer equipment and headphones where appropriate and separated by appropriate spacing or partitions
    - A suitable chair for each Candidate
    - Adequate space between Candidates to prevent cheating

Test Centre personnel shall remove all personal belongings, including communication devices, from Candidates for the duration of the Test and store them securely away from the Test room. The Concessionaire shall monitor and regulate the security and compliance of any agent, sub-contractor or

third party providing SELT testing on its behalf for the duration of the Concession Agreement.

The Concessionaire shall have a risk register for SELT Service, including a risk rating for each Test Centre.

The Concessionaire shall report risks and issues to the security and compliance of any Test Centre to the Authority through the Monthly Report or the Compromised Testing Notification appropriate to the likelihood and impact of the risk/issue.

The Concessionaire shall also evidence and make available on request all monitoring and regulation of the security and compliance required by the Authority

The Concessionaire shall monitor and regulate the security and compliance of any agent, sub-contractor or third party providing SELT testing on its behalf for the duration of the Concession Agreement.

The Concessionaire shall install and use video recording in all SELT test registration and for individual candidates taking the test.

The Concessionaire shall review an appropriate proportion of videos as part of its security checking of Test delivery.

The Concessionaire shall also securely store the recordings for a minimum of 60 days and make them available immediately at the Authority's request at any time within that timeframe.

The Concessionaire and those operating on its behalf shall check and confirm each Candidate's identity at registration, prior to them entering the Testing room and upon re-entry into the Testing room following a break.

In delivering this requirement the Concessionaire and those operating on its behalf shall ensure that:

- Any Candidates testing outside their country of origin use their passport or travel document as identification;
- Candidates' identification documents contain a photograph which matches that of the Candidate and that these documents have not expired;
- The identity documentation is checked to ensure the biographic details (name, date of birth, nationality, gender plus passport number as presented) match those in which the Test booking was made;
- Candidates' photographic ID is checked to ensure it matches the Candidate;
- a photograph is taken of the Candidate at registration on the Test day(s) and compared with the Candidate's photographic ID. This photograph shall be visible to the Authority via the Online Verification System.
- Candidates are asked at registration on the Test day to provide a sample of their signature and this is compared to that on the identity documents provided;
- A voice sample of all Candidates is taken and kept to enable later identification of any proxy testing or other irregularity using comparison to the Candidate and/or other Candidates;
- The Concessionaire shall ensure all Candidate checks are documented and are made available for the Authority on request for the Term of the Concession Agreement and for up to two years thereafter.

<Redacted>

The Concessionaire and those operating on its behalf shall use a form of secure identity management to identify Candidates:

- on the day of the Test,
- prior to releasing Test scores; and
- on subsequent Tests taken.

Should concerns be raised around possible or confirmed compromised tests, the Concessionaire shall notify the Authority immediately via the Compromised Test Notification to the SELT Mailbox. It shall then produce a report for the Authority that includes:

- Full name and address of the Test Centre(s) involved
- Test Centre number(s)
- How the issue was identified
- Candidate details of those found/suspected to be involved which shall include:-
  - Full name (as confirmed on their Government identification document)
  - Date of birth
  - Nationality
  - Passport/ID number
  - Gender
  - Full address
  - Date of test
- Confirmation of whether the Test results have been issued to the Candidate(s)
- Any cancellation and/or withholding of Test scores
- Reason(s) for cancelling Test scores
- What action is being taken to further investigate or manage the Incident
- Timescales for completion of this action

This report shall be sent to the Authority as soon as possible (and no more than one month) after the Compromised Test Notification has been completed.

The Concessionaire shall ensure that an appropriate proportion of SELT Tests are re-marked or otherwise properly re-checked to ensure quality of Test result.
The Concessionaire shall undertake appropriate checks on completed Tests prior to releasing the relevant Candidates' Test scores to satisfy itself that:

- the Test was taken by the Candidate, according to the security requirements of the Authority; and
- there was no cheating/attempted cheating; and

- the Test result is valid.

The Concessionaire shall have a security and anti corruption policy for all of its Test Centres whether directly managed or operated on its behalf by a third party. The policy shall set out the following:

- The awareness training delivered to personnel and how often this training is delivered
- Whistle-blowing policy and arrangements
- Investigations processes
- Disciplinary processes
- Staff roles and responsibilities

How incidents relating to security, integrity or possible compromised testing will be escalated to appropriate authorities

The Concessionaire must also demonstrate conformance to ISO 27001 in its:

- general security standards
- Security Operating Procedures used in the maintenance and operation of existing IT systems
- development and operation of all future IT systems; and
- day-to-day operations of Test Centres.

- Creation of a continuity plan and contingency actions in the event of security incidents, including establishment of clear responsibilities and a mechanism for handling incidents.

1. Key security elements to be included in the Concessionaire Security Plan

The six physical security elements to be included in the Concessionaire Security Plan are set out as follows:

Perimeter of Test Centre

- The Concessionaire must implement a system of prevention, detection and response to incidents, to guard against unauthorised personnel and vehicles entering the boundary of the site, both during operating hours and when the Test Centre is closed.

Building access points

- All building access points must be robustly secured, alarmed and monitored when not in use and during hours when the Test Centre is closed.

Public areas

- There must be CCTV surveillance of the public who are in Test Centre buildings
- There must be CCTV surveillance of test registration to ensure integrity of operation.

Staff and service areas

- There must be controls to prevent the public from entering staff and service areas or where cash or valuables or sensitive data are handled or stored

- Items such as candidates' supporting or travel documents must be handled and stored securely at all times

ANNEX 2.2-2 TO SCHEDULE 2.2 (SECURITY) - THE CONCESSIONAIRE'S SECURITY PLAN

[Drafting Note: Placeholder for the Concessionaire's Security Plan]

The Security Plan shall, as a minimum, include a summary and description of the policy and processes for the following areas:

1.1. *The* Concessionaire's *organisational risk assessment and treatment*
1.2. *The* Concessionaire's *security policy*
1.3. *The* Concessionaire's *information security policy and processes, including accreditations*
1.4. *Asset management*
1.5. *HR and personnel security*
1.6. *Physical and environmental security*
1.7. *Communications and operational management*
1.8. *Access control procedure*
1.9. *Information security incident management*
1.10. *The* Concessionaire's *Fraud and Anti corruption Risk Assessment*