



Home Office

AUTHORITY: The Secretary of State for the Home Department

## **SCHEDULE 10**

### **SECURITY**

#### **Provision of Adult Victims of Modern Slavery Care and Co-ordination Services**

1. The Contractor is required to adhere to specific security provisions as set out by the Authority within Clause 29 of the Contract and this Schedule including Annex Security Policy for Contracts

**2. Physical Security**

2.1 The Contractor shall ensure that, as a minimum:

- a) protectively marked data is secured in appropriate security containers;
- b) access to Authority Data is restricted to Staff who have passed the relevant Staff Vetting Procedures and have a demonstrable need to have access to Authority Data to carry out their duties.
- c) Windows, locks, doors and entry controls, CCTV, at accommodation owned or used by the Provider in connection with the provision of the Services meet appropriate security standards; and
- d) Plans are in place for dealing with and intercepting unauthorised visitors and intruders

**Accountability in respect of Authority Data**

3.1 The Contractor shall appoint at least one responsible person who is accountable for the assurance of Authority Data used in delivering the Services. The responsible person shall be named within Schedule 7 (**Key Representatives**).

3.2 The Contractor shall consult with the Authority in relation to any proposed change to the person accountable for the assurance of Authority Data.

**3. Structured Risk Assessment for Authority Data**

4.1 The Contractor shall ensure that it has undertaken a structured risk assessment which highlights when Authority Data is most vulnerable whilst in its care.

4.2 The Contractor shall ensure that:

- a) it records the security risks identified as a result of such risk assessment in a risk register with such risk register to be made available to the Authority on request;
- b) the results of such risk assessment are taken into account when planning, selecting, designing and modifying its facilities..

#### **4. Data Handling Policies**

5.1 The Contractor shall have in place documented policies and procedures which are consistent with the requirements of the Contract and which govern the delivery of the Services with respect to:

- a) the level of security clearance required by Staff before they can access Authority Data, some senior staff may need higher clearance, CTC and/or SC;
- b) where Authority Data can be stored;
- c) when Authority Data can or cannot be transmitted electronically, by fax or discussed over the telephone; and
- d) when Authority Data can or cannot be sent via post or courier.
- e) The secure disposal of data that complies with the Authority's policy.

5.2 Without prejudice to its obligations under the DPA (and Clause 26 (Protection of Personal Data)), the Contractor shall have clear policies in place which cover, as a minimum, the following principles of the DPA:

- a) Personal Data is processed fairly and lawfully;
- b) Personal Data is obtained and only used for specified and lawful purposes;
- c) Personal Data is adequate, relevant and not excessive;
- d) Personal Data is accurate and kept up to date;
- e) Personal Data is kept for no longer than is necessary;

- f) Personal Data is processed in accordance with the individual's rights;
- g) Personal Data is kept secure; and
- h) Personal Data is only transferred to countries that offer adequate data protection and where the Authority's approval has been granted and the conditions of Clause 26 have been met.

5.3 The Contractor shall have in place clear policies for informing Staff of responsibilities, restrictions and considerations when sharing access to Authority Data with other members of Staff.

5.4 The Contractor shall provide guidance to its Staff on its policies and procedures for handling Authority Data. The Contractor shall further procure that any guidance, policies, procedures and contracts placed in furtherance to the execution of this Contract with such third parties, shall, as a minimum, contain all requirements relating to the secure handling of information as set out within this Contract.

## **5. Breaches**

6.1 The Contractor shall have in place a documented procedure which addresses breaches of the requirements for handling Authority Data (including the procedures the Contractor is required by this Schedule to have in place). Any breach or suspected breach must be reported immediately to the Authority by telephone, followed by notification pursuant to Clause 55.

6.2 The Contractor shall ensure that clear guidance is provided to the Staff and any third parties it proposes to engage in the delivery of this Contract highlighting that deliberate or accidental compromise of protectively marked material may lead to disciplinary action and/or criminal proceedings.

**ANNEX 1****SECURITY POLICY**

The Contractor's Security must conform to the Home Office Security Policy for Contracts Volume 4 provided as a separate document.