

**We released this document in response  
to a Freedom of Information request.  
Over time it may become out of date.**

Department for Work and Pensions

## SCHEDULE 2

### ANNEX A

#### HOSTING SERVICES AND NETWORK OPERATING CENTRE SERVICES

##### 1. **Scope of Annex**

1.1 This Annex A details the Hosting Services, Network Operating Services and any other related Services that shall be provided by the CONTRACTOR.

1.2 For each service requirement, the CONTRACTOR shall provide the Hosting Services commensurate with the relevant Service Levels as described in Schedule 4, Annex B and the Service Level Proforma set out in Schedule 4, Annex C.

##### 2. **Scope of Hosting Services Provided**

2.1 The CONTRACTOR shall provide and manage the Hosting Services in the Data Centre *[located in the United Kingdom]*. The specific responsibilities of the AUTHORITY and the CONTRACTOR are specified below.

2.2 The CONTRACTOR shall provide the following Hosting Services.:

(A) Data Centre Space Rental Services:

(1) Information redacted

(a) Information redacted

(b) Information redacted

(c) Information redacted.

(2) Information redacted.

(3) The Data Centre will comply with the security requirements of Schedule 11 (Security) and will comply with the following security documents:

(a) overview plan of the Data Centre space showing required external security features: Information redacted; and

(b) E01 – Security Review comprising five separately controlled parts: ADS Review, Security Design and Assessment, Risk Analysis, IT Health Check Requirements and Annex A Security Requirements, all at version 4.0, dated 08 December 2005.

(4) The Data Centre shall include Internet and GSi network connectivity.

(5) The Data Centre shall have undergone a flood liability threat assessment, the results of which must be shared with the AUTHORITY on the AUTHORITY's request.

(B) Data Centre Operations Services:

- (1) The CONTRACTOR will provide the following Data Centre Operations Services:
- (a) operation of the NOC;
  - (b) backup and restore management as defined by the backup and restore procedures produced in the CCN 8 Transition Work Package;
  - (c) the Service Management Procedures as produced in the CCN 8 Transition Work Package;
  - (d) management of third party service providers as required to perform the Hosting Services;
  - (e) collaboration with the AUTHORITY in forward planning;
  - (f) collaboration with the AUTHORITY's IT Service Continuity Management and the provision of the CONTRACTOR's up to date generic ITSCM services for the **Information redacted** facility;
  - (g) provision of Management Information as specified in Schedule 4, Annex B regarding the performance and use of the Hosting Services; and
  - (h) for the avoidance of doubt, any procedures required to deliver the Data Centre Operations Services provided as part of the CCN 8 Transition Work Package and shall be maintained as part of the Hosting Services.

### 3. **Resources**

#### 3.1 **CONTRACTOR Personnel**

- (A) The CONTRACTOR shall ensure that shift staff (excluding the shift leaders) working in the NOC are dedicated to Government service provision.
- (B) The CONTRACTOR shall ensure that the Hosting Services are delivered by CONTRACTOR Personnel located at the Data Centre or at other locations agreed by the AUTHORITY.
- (C) The CONTRACTOR shall maintain the working practices specific to the provision of the Hosting Services that are in accordance with Best Practice and Schedule 4, Annex B, and to which the CONTRACTOR Personnel shall adhere.

#### 3.2 **Information redacted**

**Information redacted:**

- (A) **Information redacted;**
- (B) **Information redacted;**
- (C) **Information redacted;**

- (D) Information redacted;
- (E) Information redacted;
- (F) Information redacted;
- (G) Information redacted;
- (H) Information redacted;
- (I) Information redacted;
- (J) Information redacted.

3.3 Information redacted

Information redacted:

- (A) Information redacted;
- (B) Information redacted;
- (C) Information redacted;
- (D) Information redacted
- (E) Information redacted.

3.4 Information redacted

Information redacted:

- (A) Information redacted;
- (B) Information redacted;
- (C) Information redacted;
- (D) Information redacted
- (E) Information redacted.

3.5 Information redacted

Information redacted:

- (A) Information redacted;
- (B) Information redacted.

3.6 Information redacted

Information redacted:

- (A) Information redacted;

- (B) Information redacted;
- (C) Information redacted;
- (D) Information redacted;
- (E) Information redacted;
- (F) Information redacted.

#### 4. **Data storage**

##### 4.1 **Backups**

- (A) The CONTRACTOR shall ensure that Data is copied to tape in accordance with the backup and restore procedures produced in the Transition Work Package.
- (B) The CONTRACTOR shall ensure that the Data copied to tape is stored in a secure off-site storage facility.
- (C) The CONTRACTOR shall be responsible for retrieving tapes from the off-site storage facility. Ad hoc requests will be charged in accordance with Schedule 15 (Charges).

##### 4.2 **Disk and Media Management**

- (A) The CONTRACTOR shall establish and comply with procedures that ensure that the security of Data stored on Data Media is maintained in accordance with the provisions of the Schedule 11 (Security). The CONTRACTOR shall keep all Data Media at the Data Centre in a secure area away from the source of the backup, or at other locations agreed with the AUTHORITY.
- (B) The CONTRACTOR shall agree with the AUTHORITY and shall follow a tape movement and retention scheme that will ensure that certain specified tapes are retained for a specified period, and that some tapes are stored away from the site containing the original Data at another secure site agreed with the AUTHORITY.
- (C) The CONTRACTOR shall ensure that any Data Media that leaves the CONTRACTOR's control other than to the AUTHORITY shall be destroyed using a method defined in Schedule 11 (Security), unless otherwise authorised by the AUTHORITY.
- (D) The CONTRACTOR shall ensure that all exchangeable media arriving in the Data Centre or created by the CONTRACTOR for use in the Data Centre will pass through a formal reception procedure that shall include virus scanning and other tests as defined in the procedures delivered as part of the CCN 8 Transition Work Package.
- (E) The CONTRACTOR shall be responsible for the maintenance of the virus signatures for scanning exchangeable media.

5. **Asset and configuration control**

5.1 In addition to the requirements of paragraph 3.6 of Schedule 2, the CONTRACTOR shall provide a procedure for control of all equipment and its movement in and out of the Data Centre.

6. **Network Operations Centre**

6.1 The CONTRACTOR shall provide a NOC in the Data Centre dedicated to supporting Government systems. The NOC shall be in a secure area, and separate from the Data Hall, and shall only be accessible by authorised personnel.

6.2 The CONTRACTOR shall staff the NOC with two or more appropriately qualified and experienced CONTRACTOR Personnel on a 24x7 basis throughout the period of Hosting Services operation.

6.3 The CONTRACTOR shall undertake the following activities in the NOC:

- (A) monitor the Hosting Services and the Monitored Systems and follow documented NOC procedures for any errors, warnings or Alerts generated by the Monitored Systems;
- (B) perform Change Management that will control, record and obtain authorisation for all Changes to the Hosting Services;
- (C) perform Service Level Management and management report preparation for the Hosting Services in accordance with Best Practice and Schedule 4, Annex B;
- (D) perform Capacity Management for all aspects of the Hosting Services as defined in Schedule 4, Annex B;
- (E) perform Incident Management and Problem Management in accordance with Best Practice and Schedule 4, Annex B, and shall lead the investigation of Hosting Services issues from the NOC, as defined in the Incident Management and Major Incident Management Procedures established by the CONTRACTOR and agreed by the AUTHORITY;
- (F) manage threats identified by Security Monitors and shall follow the procedures specified in the security approvals of the site and each ADS as it applies to the Hosting Services, and the security policy established by the CONTRACTOR as defined under Schedule 11 (Security);
- (G) control physical access to the Data Hall using procedures agreed with the AUTHORITY and as defined in Schedule 11 (Security); and
- (H) utilise the AUTHORITY provided Tools according to the Service Levels.

7. **Service Management**

7.1 The CONTRACTOR shall maintain procedures to manage the Hosting Services in a way that shall achieve the Service Levels as defined in Schedule 4, Annex B and the CONTRACTOR shall comply with these procedures. The CONTRACTOR shall implement these in accordance with principles of Best Practice.

- 7.2 The CONTRACTOR shall perform Problem Management in accordance with paragraph 3.3 of Schedule 2 and Schedule 4, Annex B, including identification of the root cause of Incidents, applying fixes to resolve underlying Problems and performing proactive Problem Management, for example, performing trend analysis in Incident and Problem record data.
- 7.3 The CONTRACTOR shall perform Capacity Management and Planning in accordance with paragraph 3.8 of Schedule 2 and Schedule 4, Annex B. The CONTRACTOR shall ensure that the network component of the technical infrastructure is delivered in the right volume at the right time. The deliverables from Capacity Management and Planning are described in Schedule 4, Annex B.
- 7.4 The CONTRACTOR shall as required make recommendations to relieve potential future degradation in the performance of the Gateway and the Services and the AUTHORITY shall review the recommendations.
- 7.5 The CONTRACTOR shall collaborate with the AUTHORITY's IT Service Continuity Management and provide the AUTHORITY with standard ITSCM services for the Data Centre.
- 7.6 The CONTRACTOR shall perform Availability Management in accordance with paragraph 3.7 of Schedule 2 and Schedule 4, Annex B and to ensure that the required levels of Availability for the Hosting Services are met and that ways are identified to improve the Availability of the Hosting Services. The precise levels of Availability contracted are defined in Schedule 4, Annex B.
- 7.7 The CONTRACTOR shall perform Incident Management in accordance with paragraph 3.2 of Schedule 2 and Schedule 4, Annex B. The deliverables for Incident Management are defined in Schedule 4, Annex B.
- 7.8 The CONTRACTOR shall perform Release Management as it applies to the Hosting Services in accordance with paragraph 3.5 of Schedule 2. The deliverables for Release Management are defined in Schedule 4, Annex B.
- 7.9 The CONTRACTOR shall perform Change Management as it applies to the Hosting Services in accordance with paragraph 3.4 of Schedule 2. The deliverables for Change Management are defined in Schedule 4, Annex B.
- 7.10 The CONTRACTOR shall perform Service Level Management as it applies to the Hosting Services in accordance with paragraph 3.10 of Schedule 2. The deliverables for Service Level Management are defined in Schedule 4, Annex B.
- 7.11 The CONTRACTOR shall perform Configuration Management as it applies to the Hosting Services in accordance with paragraph 3.6 of Schedule 2. The deliverables for Configuration Management are defined in Schedule 4, Annex B.
- 7.12 The CONTRACTOR shall perform IT Service Continuity Management as it applies to the Hosting Services in accordance with paragraph 3.9 of Schedule 2. The deliverables for Configuration Management are defined in Schedule 4, Annex B.
- 7.13 The CONTRACTOR shall consider emergency Service Continuity Invocation when a prolonged loss of capability to deliver the Hosting Services is expected. The decision to invoke an ITSCM Plan shall be taken in conjunction between the CONTRACTOR and the AUTHORITY. The CONTRACTOR shall develop, agree with the AUTHORITY, and implement communication procedures to ensure that the nominated contacts within the AUTHORITY are informed about the possibility of invoking ITSCM Plans.