

# A guide for DWP contractors on the DWP Offshoring Policy v2.0

May 2011

## Overview

1. All services performed by Contractors on behalf of the Department must comply with Her Majesty's Government (HMG) policies and standards and in particular the Cabinet Office Security Policy Framework (SPF) - Mandatory Requirement 31 which mandates that Government Departments must have an Information Security Policy setting out how it and its delivery partners, including those offshore and nearshore, comply with the SPF minimum requirements.
2. In compliance with this requirement, DWP has implemented the DWP Offshoring Policy which details controls and recommended practices for those responsible for awarding and managing contracts for the Department, and Contractors or its Sub-contractor who are considering hosting or accessing Departmental Systems, Services or Official Information (also known as 'Authority Data') outside of the UK.

## Offshoring

3. The DWP Offshoring Policy controls apply when a contractor or sub-contractor wishes to:
  - host Departmental systems, services or official information outside the UK;
  - allow staff based outside the UK to have access to Departmental systems, services or official information;
  - bring foreign nationals ("Landed Resources") to the UK to provide services including, but not limited to, applications development and support, testing and other similar activities.

## Example scenarios

4. The following examples illustrate some typical offshoring scenarios:
  - A contractor or its sub-contractor staff outside the UK access DWP official information or systems hosted in the UK.
  - A contractor or its sub-contractor staff outside the UK access DWP official information or systems hosted outside the UK.
  - A contractor or its sub-contractor staff in the UK access DWP official information or systems hosted outside the UK.
  - A contractor or its sub-contractor causes foreign nationals to be brought to the United Kingdom, for the purpose of delivering services to the Department in the UK, and these members of staff have access to DWP official information or systems.
5. The following examples are **not** offshoring:
  - A contractor or its sub-contractor provides services to the Department, and systems or data is hosted outside the UK but this does not include DWP official information or systems.

- A contractor or its sub-contractor provides services to the Department, and this involves contractor or its sub-contractor staff outside the UK, but these staff do not have access to any DWP official information or systems.
- A contractor or its sub-contractor causes foreign nationals already living in the UK to provide the services.
- A contractor or its sub-contractor causes foreign nationals to be brought to the UK, for the purpose of delivering services to the Department, and these members of staff do not have any access to DWP official information or systems.

## **Offshoring process and approval**

6. Offshoring (including Landed Resources) is subject to the DWP Offshoring Approval Process. This process ensures that the Department is sighted on instances of offshoring and allows an assessment of risk to be made. The contractor is responsible for informing DWP prior to offshoring any services which include access to or storage of Departmental official information and systems.
7. A contractor can request approval by initially submitting a completed DWP Offshore Proposal Questionnaire (Appendix A) to their Contract Manager, for assessment by the Departmental Security Team.
8. If tenderers are planning to offshore they will be required to complete the DWP Offshore Proposal Questionnaire and include with their bid. Additional information may be sought by DWP Departmental Security Team.
9. In all cases approval must be obtained from DWP's Security Team prior to the commencement of any offshoring. Contractors who fail to inform DWP prior to offshoring may be in breach of their contract and action will be taken on a contract by contract basis.
10. The DWP offshoring approval process requires a comprehensive technical risk assessment to be performed to determine the nature and level of security controls to be applied to offshored DWP business.
11. The decision to decline an offshoring proposal will be risk based, and where ever possible the Department will take all reasonable steps to work towards an acceptable proposal with the contractor.

## **Sub-contractor assurance**

12. The lead contractor is responsible for informing DWP and seeking offshoring approval from DWP prior to commencement of sub-contractor offshoring.

# Appendix A - DWP Offshore Proposal Questionnaire

The following information is required when notifying the Department of an intention to offshore. This information will allow the Department to determine the process that is required to approve the offshoring proposal. Approval must be granted prior to the commencement of any offshore activity (including landed resources).

## 1. Description of business to be offshored

[Guidance: please provide a summary description of the work that is to be offshored in business terms.]

### 1.1 Timescales and releases

[Guidance: for development and testing activities, or other work of a limited lifecycle, please estimate the timeframe for the offshore work, and the relevant releases/phases for the systems involved.]

### 1.2 Number of staff

[Guidance: please provide the estimated number of offshore staff who will be involved in this work, and describe their different roles.]

## 2. DWP information, systems or services

[Guidance: please provide details of the DWP information, systems or services including expected quantities. Include the accreditation or assurance status of each system or service if known.]

### 2.1 Solution details

[Guidance: please describe the method of working that is proposed. This should be provided principally in terms of the DWP information, systems or services involved, and how they are handled, stored, viewed, protected, etc.

The aspect of DWP information, systems or services storage should consider permanent storage (such as a designated long-term repository), temporary storage (such as working on a checked out file before checking it back in), and transient storage (such as short term residence in communication devices)...

### 2.2 Network

Guidance: please provide details of the network at the offshore locations, and of any network connectivity used to transfer DWP information, systems or services to and/or from the offshore locations. Where possible, please provide diagrams that show where these are stored and transferred in terms of these networks.]

## **2.3 Processes and systems used across sites**

[Guidance: please describe how the procedures and systems used by offshore staff interact with those onshore.]

## **3. Offshore locations**

### **3.1 Addresses**

[Guidance: please provide the full address of the offshore locations.

Where home-working is proposed, please provide the estimated number of home workers, and also describe the process for managing home- workers.

Note that the actual addresses of home-workers need not, and should not, be provided.]

### **3.2 Other work at the sites**

[Guidance: please provide a description of any other DWP work, and any non-DWP work, that is conducted at the sites. If this information cannot be provided, then please describe how the DWP can be assured that any other work at the sites will not compromise their security.]

### **3.3 Staff clearance**

[Guidance: please provide details of the security clearance and employment checks for staff at the offshore locations. This should consider all staff at the site and not just those directly involved in the proposed work.]

## **4. Legal assessment**

[Guidance: please identify any known local conditions that may impact the security of the Department's information, systems or services or the enforcement of security requirements. Also detail whether there are any legal constraints, which need to be considered such as:

- computer misuse
- use of encryption
- confidentiality statements
- if personal information (staff or customer) is to be stored or accessed in the offshore location, then the contractor must also provide details of arrangements made to ensure that comparable protection is provided as required by the Data Protection Act 1998 (e.g. safe harbour agreements)"]

## 5. Governance

Role	
Name	
Responsibility	
Organisation	
Contact details	
Address	
Tel no	
E-mail	

[Guidance: Please identify the person within the contractor organisation with responsibility for the offshoring. This person may be required to provide additional detail to support the offshoring request, and may be contacted directly by the Departmental Security Team.]