Contracting Authority Security Policies and Standards

1. The Department for Work and Pensions (DWP) treats information as a valuable asset and considers that it is essential that information must be protected, together with the systems, equipment and processes which support its use. These information assets may include data, text, drawings, diagrams, images or sounds in electronic, magnetic, optical or tangible media, together with any Personal Data for which DWP is the Data Controller.

2. In order to protect DWP information appropriately, our Contractors must provide the security measures and safeguards appropriate to the nature and use of the information. All Contractors of services to DWP must comply, and be able to demonstrate compliance, with the relevant DWP policies and standards.

3. The main DWP policies include:-

   - Information Security Policy
   - Physical Security Policy
   - Acceptable Use Policy

   The above policies can be found at: gov.uk

4. Each Contractor must appoint a named officer who will act as a first point of contact with the Department for security issues. In addition all Staff working for the Contractor and where relevant Sub-contractors, with access to DWP IT Systems, Services, DWP information or DWP sites must be made aware of these requirements and must comply with them.

5. The policies and requirements are based on and follow ISO27001 and Cyber Essentials, but with specific reference to DWP use.

6. Whilst Departmental policies are written for internal Departmental requirements all Contractors must implement appropriate arrangements which ensure that the Department's information and any other Departmental assets are protected in accordance with prevailing statutory and government requirements. These arrangements will clearly vary according to the size of the organisation so should be applied proportionately.

7. It is the Contractor's responsibility to monitor compliance of any Sub-contractors and provide assurance to DWP as requested.

8. Failure to comply with any of these Policies and Standards could result in termination of current Contract.

9. The following are some key basic requirements that all Contractors must apply:

10. Personnel Security

10.1 Staff recruitment in accordance with government requirements for pre-employment checks; including Baseline Personnel Security Standard.

10.2 Staff training and awareness of DWP security and any specific contract requirements.

11. Secure Information Handling and Transfers

11.1 Physical and electronic handling, processing and transferring of DWP Data, including secure access to systems and the use of encryption where appropriate.

12. Portable Media

12.1 The use of encrypted laptops and encrypted storage devices and other removable media when handling DWP information.

13. Offshoring

13.1 DWP data must not be processed outside the United Kingdom without the prior written consent of DWP and must at all times comply with the Data Protection Act 1998.

14. Physical Security

14.1 Security of premises and control of access.

15. Security Incidents

15.1 Includes identification, managing and agreed reporting procedures for actual or suspected security breaches.

Draft Security Plan

SA Security Plan.xls