DWP Security Policy for Contractors

The Department for Work and Pensions treats its 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 the Department for Work and Pensions is the Data Controller.

In order to protect Departmental information appropriately, our suppliers must provide the security measures and safeguards appropriate to the nature and use of the information. All suppliers of services to the Department for Work and Pensions must comply, and be able to demonstrate compliance, with the Department's relevant policies and standards.

The Chief Executive or other suitable senior official of each supplier must agree in writing to comply with these policies and standards. Each supplier must also 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 supplier and where relevant sub-contractors, with access to Departmental IT Systems, Services or Departmental information must be made aware of these requirements and must comply with them.

All suppliers must comply with the relevant DWP Standards. The Standards are based on and follow the same format as ISO27001 and Cyber Essentials, but with specific reference to the Department's use.

The following are key requirements and all suppliers must comply with relevant DWP policies concerning:

Personnel Security

- Staff recruitment in accordance with government requirements for pre-employment checks;

- Staff training and awareness of Departmental security and any specific contract requirements.

Secure Information Handling and Transfers

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

Portable Media

- The use of encrypted laptops and encrypted storage devices and other removable media when handling Departmental information.

Offshoring

- The Department's 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.

Premises Security

- Security of premises and control of access.

Security Incidents

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

All suppliers must implement appropriate arrangements which ensure that the Department's information and any other Departmental assets are protected in accordance with prevailing statutory and central government requirements. These arrangements will clearly vary according to the size of the organisation.

It is the supplier's responsibility to monitor compliance of any sub-contractors and provide assurance to DWP.

Failure to comply with any of these Policies or Standards could result in termination of contract.

For enquiries please contact The Supply Chain Information Assurance Team on:

SUPPLYCHAIN.INFORMATIONASSURANCETEAM@DWP.GSI.GOV.UK