Department for Work & Pensions

Supplying to DWP

(July 2016)

Data Protection and Security of Information in DWP

Data Protection and Assurance

In support of Government policy and Data Protection requirements DWP work very closely with suppliers to understand and apply relevant measures to protect data. DWP seeks to develop safeguards in all of its relationships and continually updates guidance for our commercial contract and performance managers to help them evaluate and manage risk to data in contracts.

This activity with suppliers is now very evident in reporting and the development of contract specific security plans. The review and evaluation of risk to information in contracts is a fundamental step in action to reduce and address data protection requirements. DWP actively seeks evidence based assurance from suppliers that measures and controls to safeguard data can be demonstrated.

DWP uses a variety of methods to give assurance that suppliers and delivery partners are meeting the standards outlined in this note, and the more detailed requirements on data security which are contained within contracts. DWP will ask for information on specific controls employed to protect data, and DWP or our appointed agents can carry out audits and a programme of visits and spot checks to confirm.

The risk of loss of public confidence through failure to protect sensitive or personal information remains a key risk for DWP. Many of you will be aware of the powers of the Information Commissioner to impose fines following significant data losses.

DWP endeavour to improve and continue to develop with you the processes and controls necessary to protect the data that is so important to our business.

Your actions with DWP to date have ensured that no major loss of data has occurred in delivery of our business, and where incidents have been identified that they have been managed openly and decisively. By avoiding complacency, working in close partnership and understanding the need to protect data we can continue to maintain customer confidence.

Please use assurance as a positive way of promoting data security, and consider carefully how you can assure yourselves, and us, that our data is protected.

Whether high or low volumes

DWP has millions of customers, and around 85,000 staff. Our business is about people, and DWP regard their personal data as a valuable and sensitive asset which has been entrusted to us.
DWP therefore take data protection extremely seriously, and require our suppliers (and their supply chain) to apply the high standards that DWP themselves apply.

You have a responsibility to protect data

You must be clear who in your organisation is responsible for assuring you that the organisation is compliant with the Data Protection Act. You should find out what awareness of the data protection principles exists among your key staff, and if the level of awareness is not adequate you should put in place a programme to raise it. Information can be found at the Supplying DWP internet site.

You must ensure that anything you do with our data – whether storing, copying, sharing, communicating or transmitting it – is both lawful and secure. The starting point is that you should do

nothing with the data without our knowledge and authority. In particular if you wish to use the data for a purpose that is different to the purpose for which we gave it to you, you must seek permission first. Legislation requires us to operate appropriate technical and organisational measures to keep information safe, and we are required to place that obligation on suppliers and the supply chain.

Results and findings from supplier compliance visits

DWP monitoring teams conduct on-going compliance review programmes to ensure that suppliers and their supply chain have appropriate controls and measures in place to protect data. Specific controls are agreed for each contract and adherence to contractual requirements as well as Data Protection principles are established via these checks. Our monitoring programmes are used not only to confirm measures are in force and updated, but to further improve supplier and DWP's processes for control of data.

Recommendations are produced and good practice shared. Key areas for suppliers to put in place are measures to ensure that all portable media devices are appropriately encrypted: that employees who access data or assets are vetted to the required level (HMG Baseline Personnel Security Standard): that clearly defined data access levels are operated for your staff: that access is controlled and removed where necessary.

At the end of your contract you must ensure that ay records retained are protected, stored safely, accessible, and subsequently destroyed or returned to DWP in accordance with data requirements and any measures specified in your contract.

Through life measures: data must be protected throughout its business use lifecycle.

Your organisation must have clear evidence of through life controls and measures including those shown below to ensure the protection, availability and integrity of data.

Organising Information Security

The organisation must have an Information Security Policy. The Information Security Policy is a working document that is regularly updated and is applied throughout the organisation and its supply chains. The organisation must clearly articulate in policy documents its approach to comprehensive and effective information risk management and how compliance throughout the organisation and its delivery chain is to be achieved.

The organisation must have policies and processes in place for reporting, managing and resolving Information Assurance (IA) incidents. The organisation responds effectively to all IA incidents taking timely and decisive real-time action to limit the immediate business impact and by subsequently enacting preventative measures, prevents their recurrence. These incident management policies and processes make a clear distinction between what is required for post-event response and what is required to manage a real-time event.

Staff Training, Awareness and Understanding

General staff **awareness** of the need to provide effective protection to DWP information, specifically, but not exclusively, personal data, has been heightened. This applies to the members of the organisation and to those within the supply chain that have access to the organisation's information.

General staff **understanding** of the need to provide effective protection for the information remains at a level that meets the needs of the business. All members of staff within the organisation, and its delivery partners must receive adequate **training** in their responsibilities with regard to protecting the Confidentiality of DWP information.

Members of the organisation, and those within the supply chain who have access to DWP information, must demonstrate an understanding of the requirement for effective Information Assurance controls (in terms of Confidentiality, Integrity and Availability). Realistic plans are in place to implement through-life IA controls in a co-ordinated way across the organisation and its delivery chain.

Staff who have IA management responsibility and those who manage or maintain the secure configuration of ICT systems have targeted education and training.

The organisation makes use of an effective security checking and/or vetting process that is appropriate to the needs of the business and applies this before access is given to the DWP information. When any staff move within, or leave the organisation, their access rights to information or assets are removed.

The organisation has assurance that staff within the organisation, and its delivery partners who have access to the organisation's ICT systems, only use them for authorised purposes.

System Security

IA is embedded within the IT Service Management procedures for all business critical ICT Systems and this includes effective configuration management.

The organisation is aware of the need to address digital continuity. Appropriate policy is in place that addresses digital continuity and a plan exists to assess the business risk.

Penetration testing is undertaken and plans are put in place to determine ICT system vulnerabilities on a systematic basis, particularly for new ICT systems.

The organisation has a patching policy and patching is applied in a timely manner.

The risk posed by the re-use or disposal of ICT equipment and electronic media which has been used for protected information or by the disposal

of protected information in paper form is minimised within the organisation and its delivery chain by the effective application of compliant controls.

The risk to ICT systems processing protectively marked information is assessed on an annual basis.

Appropriate Business Continuity & Disaster Recovery measures are in place for ICT systems and key weaknesses are addressed.

The organisation has thorough and compliant identification and authentication controls in place on ICT systems.

The organisation has a malicious software policy, which is applied to ICT systems.

Remote Working

A policy is in place covering remote working within the organisation and its delivery partners. The Policy is based on effective control measures which are designed to reduce the risk to DWP information to an acceptable level. The organisation has assurance that the policy and **controls are effective.**

And....

The organisation has accurate details of which information assets it must retain to meet its statutory, contractual obligations and its business needs.

The organisation has implemented physical security measures to protect its information in whatever form it exists throughout its delivery chain and these measures have been tested.

The organisation has assurance that the controls governing the reuse and disposal of electronic equipment and media and the destruction of **paper based information are effective.**