DWP Department for Work and Pensions

October 2008

Dear Supplier,

**PROTECTING DWP CUSTOMER DATA AND OTHER SENSITIVE INFORMATION**

As you will know, DWP, and the Government more widely, has been reviewing and strengthening security controls and procedures to ensure effective protection of personal and sensitive information. Recent well-publicised incidents involving, for example, the loss of data held on USB memory devices have served to remind us of the importance of continuing vigilance and compliance with mandatory protective measures. The recent review by the Cabinet Office earlier this year (the results of which have been published as Data Handling Procedures in Government June 2008) introduces a number of mandatory requirements, together with a revision to the OGC model contracts in respect of security and information assurance.

The Department and your company are both under legal obligations to safeguard the information entrusted to us, and we are entitled to look to you to ensure that personal and sensitive information remains properly protected. The Information Commissioner's Office has recently indicated their expectation that "companies must introduce adequate security procedures and safeguards, for example password protection and encryption, to protect personal information before it is allowed to leave the premises on a laptop". The Department has a similar expectation in respect of all other removable electronic/magnetic media, such as USB sticks, CD ROMs, etc.

DWP attaches the utmost importance to its obligations to protect customer, staff and other sensitive information[1] – regardless of the media used to store that information. We have already taken a number of steps within the Department to ensure that any storage and transfer of information is strictly controlled and that processes are in place to protect information at all times.

These mandatory measures include:

- the use of approved encryption controls for protecting DWP data held on all removable forms of memory-storage devices, including laptops, CDs and USB memory sticks;
- the use of approved encryption controls for protection of electronic transfer of DWP data;
- the use of approved controls for protection of physical transfer of DWP data;
- the withdrawal from use of all non-encrypted USB memory sticks;
- security awareness training for all employees; and
- formal ongoing assurance of compliance with mandated protective measures.



[1] Customer, Departmental, Staff and other sensitive information referred to below as 'DWP data'.

You are required both under your contract with the DWP and the Data Protection Act to ensure security of data, we believe that recent incidents have demonstrated that these obligations can only be fully met by complying with the above best practice.

Our clear expectation is that all DWP service providers, and third parties employed by them who handle DWP data, will meet, and provide assurance of compliance with, these same standards. In particular, we would want to be assured that any DWP data provided to your organisation will continue to be stored securely for the retention period required under your contract.
*Alternative*
*"to be returned to DWP at the end of any assignment or contract or, where this has been agreed by DWP, evidence will be provided that all data and copies of such data have been destroyed in a controlled and appropriate manner".*

I would be grateful if you would confirm that your organisation is meeting all of these standards and provide me also with an assurance that these measures are subject to regular compliance review at Board level. I would be grateful if these assurances could also cover any third parties used by your organisation who have access to DWP data.

I can equally provide you with assurances that, where your organisation entrusts information to DWP, it will be subject to the same stringent controls that we apply to our own information.

It would be helpful to have your response by 20th October.

**Contact manager**