

## **NLAWARP White Paper Number 4**

### **Implementing Data Handling for Central Government**

The Government report on handling data has now been published and the data handling procedures in the document have been implemented within Central Government departments. This document and its procedures have been shared with the Local Government Association who will produce their own data handling procedures and directives by the end of the summer. It is widely anticipated that these will closely resemble those now adopted by Central Government.

The reference points in brackets give you the page and section number in the final version of the Data Handling report.

We have tried to lay this summary out in a logical sequence as follows:

- COMPLIANCE
- REPORTING
- ACCOUNTABILITY
- ENFORCEMENT
- OBLIGATORY ACTIONS
- THE GOVERNMENTS TIMETABLE

The Local Government guidelines for England and Wales, focus on;

- People
- Places
- Processes
- Procedures

This paper is a summary of the key action points laid out in the main report.

## **COMPLIANCE**

An organisation's compliance with the Data Handling rules will be closely monitored by:

- Stronger accountability mechanisms, recognising that the individual department or agency is best placed to understand and address risks to their information, including personal data.
- Stronger scrutiny of performance, to build confidence and ensure that lessons are learned and shared.

(Ref: Point 7 Page 7).

## **REPORTING**

### **YOU MUST PUBLISH FINDINGS IN YOUR ANNUAL REPORT**

- Increasing visibility of performance, with Departments publishing material in their annual reports.

(Ref.1.8 Page 12)

#### **TO INCLUDE**

- A summary of protected personal data related incidents formally reported to the Information Commissioner
- A summary of centrally recorded protected personal data related incidents not formally reported to the Information Commissioner
- A summary statement of actions to manage information risk.

(Ref. 2.42 Page 27)

## **ACCOUNTABILITY**

### **SOMEONE NEEDS TO OWN THE SECURITY RISK**

Every system has to have a single Senior Responsible Owner (SRO). The SRO is responsible for the business case and ensuring that the system achieves its aims. The SRO does this through management of the associated risks by ensuring that the right controls and protections are built in and monitored so that participating organisations can use it with confidence.

(Ref. 2.26 Page 21)

Departments cannot take responsibility for how others send information to them, although they can encourage good practice, and potentially refuse to accept material that is not handled safely.

(Ref 2.8 page 18)

## **ENFORCEMENT**

### **NEW POWERS FOR THE DATA COMMISSIONER**

- Commitment by Government to provide the Information Commissioner with new powers to conduct “spot checks”, and to introduce new sanctions under the Data Protection Act for the most serious breaches of its principles.

(Ref: 8 Page 6)

### **TARGETED INTERVENTION**

- By Departments and CESG

(Ref: 10 Page 7)

### **YOU CAN BE FINED PERSONALLY**

The Government has already introduced a new monetary penalty in the Data Protection Act (sections 55A to 55E). These ensure that data controllers who do not take reasonable steps to avoid the most serious breaches of Data Protection Act principles may be subject to a fine as well as to an enforcement notice.

(Ref: 1.15 Page 11)

### **CONTRACTORS ALSO INCLUDED**

#### **The same standards will be applied to contractors.**

Many Government Departments engage with private sector companies to contract out elements of the services they provide. Contractors will, as part of their service provision, handle information belonging to the Department or to the public for whom the Department serves.

Departments will build into new contracts the new requirements set out in this report. These requirements will also apply to existing contracts.

(Ref: 3.5 Page 27)

The Office of Government Commerce (OGC) is updating the security clauses within its model ICT contract for services, which Departments will use to provide assurance that any contractor will have processes in place which comply with the new cross-Government requirements.

(Ref: 3.6 Page 27)

### **PERSONAL DATA IS CLEARLY DEFINED**

The Information Commissioner, specified an intermediate category of information, referred to as “protected personal information”.

This definition relates to any material that links an identifiable individual with information that, if released, would put them at significant risk of harm or distress, or alternatively any source of

information relating to 1000 or more individuals that is not in the public domain, even if the information about an individual is not considered likely to cause harm or distress. As in other areas, this is a minimum baseline. Departments will often wish to apply protection to smaller data sets depending on their risk assessment and the context in which information is kept.

(Ref: 2.2 Page 17)

**IF YOU HOLD DETAILS ON MORE THAN 100,000 INDIVIDUALS YOU MUST USE AN EXTERNAL PENETRATION TESTER**

To test protections of IT systems against external attack, Departments whose delivery chain involves the handling of information relating to 100,000 or more identifiable individuals will use independent experts to conduct penetration testing.

(Ref: 2.5 Page 17)

**YOU MUST CONTROL ACCESS TO YOUR DATA AND ONLY GIVE ACCESS AFTER TRAINING.**

Strong common standards and controls are needed to control access to IT infrastructure.

Business managers are required to evaluate and declare appropriate access rights for each role in their areas and review those rights regularly.

*New members of staff are provided with access rights only on successful completion of training and minimum access rights are issued as a default.*

(Ref: 1.26 Page 12)

**OBLIGATORY ACTIONS TO BE PUT IN PLACE**

**ENCRYPTION AND PENETRATION TESTING**

Introduce obligatory use of protective measures (such as encryption and penetration testing)

(Ref: 9 Page 6)

**TRAINING**

There will be mandatory risk awareness training for those with access to protected personal information or involved in managing it.

(Ref: 2.14 Page 19)

Alongside new action to make clear that any failure to apply protective measures is a serious matter potentially leading to dismissal.

(Ref: Blue box summary Page 19)

The Cabinet Office will provide a minimum specification for this training, and seek views from Departments as to whether they would wish to use a standardised training product. The aim should be to develop training material that can be externally accredited and transferred between organisations, and integrate similar material into relevant courses run by external bodies.

(Ref: 2.16 page 20)

### **ISO MAY DISTRACT YOU FROM MORE IMPORTANT ISSUES**

Many Departments will, as now, work towards or achieve external ISO accreditation for some or all of their information systems, *but independent input to this work suggested that systematic external accreditation would absorb effort that would be better used in a more targeted way.*

(Ref: 2.2 Page 21)

### **GOVERNMENT TIMETABLE**

Departments' first full annual assessments will be **completed for the year 2008/09** and reflected in Statements on Internal Control.

(Ref 2.24 Page 21)

**By end April 2008**, all Departments had completed initial measures for the protection of personal data.

(Ref. Annex II Page 34)

#### **Departments are currently:**

- completing roll-out of new protection through their delivery chains, where they can require the use of particular measures
- putting plans in place to encourage use of protective measures where they cannot require their use

(Ref. Annex II Page 34)

**Implementation has started.**

All Departments have established new technical protections for information they hold directly.

They have identified the protected personal data they hold, are rolling out encryption to protect it in transit, and have minimised the use of removable media. (Ref 3 Page 28)

Introduced new arrangements where needed for secure disposal from the Department of paper and electronic records, and reviewed procedures for reporting information risk incidents.

(Ref. Annex II Page 34)

**Departments are currently (June 2008) undertaking a further set of activities, including:**

- appointing Information Asset Owners
- formalising their information risk policy, to reflect these new policies
- amending HR policies and guidance as necessary
- introducing cultural change plans
- publishing Information Charters; and

(Ref. Annex II Page 34)

**From July 2008:**

New systems containing protected personal data will be subject to mandated accreditation and build in greater access control and logging.

Standard contract clauses on information assurance will be incorporated into contracts.

Penetration Testing will be in place.

(Ref. Annex II Page 34)

**By the end of October 2008:**

Departments will have started their mandatory training. This timing is to allow them to develop and tailor materials as needed.

**During 2008 and 2009:**

They will have deployed the use of penetration testing.

The first full annual assessments of progress will take place following the end of 2008/09 and be reflected in the first annual Cabinet Office Report on overall progress.

(Ref. Annex II Page 34)

**encription limited are TIGER certified penetration testers**, we already provide IT Security services to several Local Authorities and would welcome the opportunity to provide both references and a competitive quotation for your IT Security requirements.

**Produced by: AAJ McDowell  
Encription Limited  
Encription House  
White Lodge  
Bever  
Worcester  
WR3 7RQ**



NLAWARP PO Box 6733 Chingford, London E4 8UD Tel: 020 8524 2185  
[www.nlawarp.gov.uk](http://www.nlawarp.gov.uk) Contact: [mark.brett@socitm.gov.uk](mailto:mark.brett@socitm.gov.uk)

© 2008 Copyright of this document is owned jointly by Socitm and encription

Non-Commercial and Public sector organisations may reproduce the contents of this document, so long as the source and copyright owners are acknowledged.