Our ref:
Your ref:

HA Board Directors

cc: Divisional Directors
Heads of Division

From: Denise Plumpton
Information Directorate
C6/04
5 Broadway
Birmingham
B15 1BL

Direct Line: 0121 687 4130
GTN: 6189 4130

2 October 2008

CIO MEMO 05/08
CONTRACTS INVOLVING PERSONAL DATA

Issue

1. All new HA contracts must have suitable provisions for data handling and data security. For the avoidance of doubt, this applies to all Agency contracts with external parties, including MACs, traffic technology work, road construction contracts, contracts for temporary staff, consultancy services and so on. No contracts are exempt from these considerations.

Background

2. A number of high-profile incidents involving the loss of personal data have led the Cabinet Office to issue guidance on data handling. The role of "Information Asset Owners" (IAOs) was introduced in CIO Memo 04/08 and this is currently being extended throughout the Agency. The Cabinet Office is also developing guidance on the inclusion of appropriate wording in contracts with external suppliers where personal data is involved. This CIO memo provides interim advice for all those who are involved in the preparation of contracts and should be cascaded to appropriate staff within your Directorates.

Action Required

3. While new guidance on contracts involving data is being prepared, DfT (C) have requested that anyone involved in negotiating a contract seeks guidance on a case by case basis. This is because we need to ensure that contracts take account of the recent Cabinet Office report on data handling which sets out new mandatory measures to improve data security (see Annex A).

4. As a result, if you are involved in, or are about to start, contract negotiations that will involve a supplier of any sort being contracted to process/handle/transfer/access any of the Agency's data, you are advised to address the following points:

   a) First establish exactly what data or information you wish the supplier to collect/hold/access/process/transfer on behalf of the Agency (e.g. anonymised, non-personal, protect personal etc);

b) If you have not yet invited tenders, you should ensure that any tender documents and specifications make reference to the protections that are required to be in place for such data. You should consider asking tenderers to specify in their response their proposals for assuring data security. Procurement contact points can advise further on this.

c) Once you have chosen your supplier, it is important to ensure there is clarity on both sides over the safeguards in place to protect data (see mandatory measures in Annex A). Appropriate wording and contract clauses should be inserted into contract documents. For advice on this speak to Procurement and Legal advisors.

d) Any data collected or processed on the Agency's behalf should be owned by an Information Asset Owner (IAO) who is a Divisional Director or HAB Direct Report. The IAO cannot be someone working for the contractor. If the data being collected is a new dataset, you must identify the IAO. For further advice on this please contact the Information Policy Team by email to the Records Management Advice inbox or call Kevin Davies on 0771314 6387 or at Kevin.davies@highways.gsi.gov.uk. Any new IAO must get in touch with the Information Policy team for further advice and training on their specific duties.

e) Once the contract is awarded and a contract manager is appointed, they should also be responsible for satisfying themselves that appropriate information security and assurance measures are in place. The IAO will also be required to provide quarterly assurance reports

Next Steps

5. With DfT colleagues, we are seeking further clarification on appropriate OGC contract clauses for information security and assurance from the Cabinet Office and working with the Procurement Directorate in order to issue further guidance as quickly as possible. In the meantime we stand ready to offer advice on a case by case basis.

Denise Plumpton

Denise Plumpton
Director of Information

Annex A – Cabinet Office Mandatory minimum measures

Government has put in place a core set of minimum mandatory measures to protect information, to apply across central Government. They are minimum measures in that they oblige individual Departments and agencies to assess their own risk, and those organisations will often put in place a higher level of protection. They will be updated in the future to accommodate lessons and new developments. This annex sets out the initial material agreed by all Departments.

III.1. Information is a key asset, and its proper use is fundamental to the delivery of public services. The public are entitled to expect that Government will protect their privacy and use and handle information professionally. Departments are best placed to understand their information and to protect it, but need to do so within a context of clear minimum standards ensuring protection of personal information.

III.2. This document sets out in Section I mandatory process measures to ensure that Departments identify and manage their information risks. In Section II it sets out mandatory specific minimum measures for protection of personal information. It does not cover physical and personnel security or business continuity, which are addressed in the Manual of Protective Security, which is under review. Departments must also comply with other obligations, such as those under contracts, codes of connection, and the law. The material in this document reflects good practice as set out in the ISO/IEC 27000 (Information Security Management System) series.

Section I: Process measures to manage information risk

General

III.3. Departments are responsible for managing their own information risks and ensuring proper management of information risks in their delivery chains, subject to meeting the mandatory rules set out in this document and its replacements. The Accounting Officer has overall responsibility for ensuring that information risks are assessed and mitigated to an acceptable level. They sign the annual Statement of Internal Control. From 08/09 onwards, this must explicitly cover information risk.

III.4. All Departments must:

4.1 have an information risk policy setting out how they implement the measures in this document in their own activity and that of their delivery partners, and monitor compliance with the policy and its effectiveness;

4.2 assess risks to the confidentiality, integrity and availability of information in their delivery chain at least quarterly, taking account of extant Government-wide guidance, and plan and implement proportionate responses, which must at least include implementation of the measures in Section II. At least once a year, the risk assessment must examine forthcoming potential changes in services, technology and threats;

4.3 accredit ICT systems handling protectively marked information to the Government standard, and to reaccredit when systems undergo significant change, or at least every five years;

4.4 conduct Privacy Impact Assessments so that they can be considered as part of the information risk aspects of Gateway Reviews, or while going through accreditation if no Gateway has been conducted for a particular system;

4.5 use the security clauses from the Office of Government Commerce's model ICT contract for services, with any changes relevant to information risk being approved by the SIRO (defined below);

4.6 consider whether each Section I measure needs to be applied to any organisation handling information on its behalf (whether public sector or private sector) to ensure appropriate information handling across the delivery chain, and apply those where there is a need to do so;

4.7 apply all Section II measures by organisations handling information on their behalf

when they deal with Government data, and monitor the application of those measures. When seeking to apply Section I or Section II measures, Departments must insist on action where they can, and seek to influence others where necessary.

Roles

III.5. All Departments must:

5.1 name a board member as "Senior Information Risk Owner" (SIRO). The SIRO is an executive who is familiar with information risks and the organisation's response. The SIRO may also be the Chief Information Officer (CIO) if the latter is on the board. They own the information risk policy and risk assessment, act as an advocate for information risk on the board and in internal discussions, and provide written advice to the accounting officer on the content of their Statement of Internal Control relating to information risk;

5.2 identify their information assets, and name for each an "information asset owner". Asset owners must be senior individuals involved in running the relevant business. Their role is to understand what information is held, what is added and what is removed, how information is moved, and who has access and why. As a result they are able to understand and address risks to the information, and ensure that information is fully used within the law for the public good. They provide a written judgement of the security and use of their asset annually to support the audit process; and

5.3 identify and keep a record of those members of staff and contractors with access to or involved in handling individual records containing protected personal data (see attachment A), referred to below as "users". For simplicity, some Departments may wish to assume that all staff are users, or to conduct the exercise for their organisation piece by piece.

Maximising public benefit from information

III.6. Addressing information risk involves ensuring that information is used, as well as protecting it when it is used. Information asset owners must consider on an annual basis how better use could be made of their information assets within the law. Where they consider that public protection or public services could be enhanced through greater access to information held by others, they should submit a request to the relevant information asset owner. Requests received must be logged and considered. Where it is decided that public access to information is in the public interest, information asset owners should reflect this in their Departmental Freedom of Information Publication Scheme.

Audit

III.7. All Departments must:

7.1 share and discuss the information risk assessment (see 4.2) with their audit committee and main board;

7.2 conduct at least an annual assessment of information risk for the SIRO to support their written advice to the Accounting Officer. That assessment must cover the effectiveness of the overarching policy. It must be informed by the written judgement of the information asset owners, and chair of the audit committee; and

7.3 once the Statement on Internal Control has been completed, share the relevant material and the supporting annual assessment with Cabinet Office.

Culture

III.8. All Departments must:

8.1 have and execute plans to lead and foster a culture that values, protects and uses information for the public good, and monitor progress at least though standardised civil-service wide questions when conducting a people survey or equivalent;

8.2 reflect performance in managing information risk into HR processes, in particular making clear that failure to apply Departmental procedure is a serious matter, and in some situations amount to gross misconduct; and

8.3 maintain mechanisms that command the confidence of individuals through which they may bring concerns about information risk to the attention of senior management or the audit committee, anonymously if necessary, and record concerns expressed and action taken in

response.

Incident management

III.9. All Departments must:

9.1 have a policy for reporting, managing and recovering from information risk incidents, including losses of protected personal data and ICT security incidents, defining responsibilities, and make staff aware of the policy; and

9.2 report security incidents to HMG's incident management schemes (GovCERTUK for network security incidents and CINRAS for incidents involving cryptographic items). Significant actual or potential losses of personal data should be shared with the Information Commissioner and the Cabinet Office.

Transparency

III.10. All Departments must:

10.1 publish an information charter setting out how they handle information and how members of the public can address any concerns that they have;

10.2 set out in the Departmental annual report summary material on information risk, covering the overall judgement in the Statement on Internal Control, numbers of information risk incidents sufficiently significant for the Information Commissioner to be informed, the numbers of people potentially affected, and actions taken to contain the breach and prevent recurrence.

Section II: Specific minimum measures to protect personal information

III.11. Government must be particularly careful to protect personal data whose release or loss could cause harm or distress to individuals. All Departments must:

11.1 determine what information they or their delivery partners hold that falls into this category. This must include at least the information outlined at A; and

11.2 handle all such information as if it were at least "PROTECT – PERSONAL DATA" while it is processed or stored within Government or its delivery partners, applying the measures in this document. Information should continue to be marked to a higher level where that is already done or where justified for example as a result of aggregation of data.

Preventing unauthorised access to protectively marked information

III.12. When PROTECT level information is held on paper, it must be locked away when not in use or the premises on which it is held secured. When information is held and accessed on ICT systems on secure premises, all Departments must apply the minimum protections for information set out in the matrix at B, or equivalent measures, as well as any additional protections as needed as a result of their risk assessment. Where equivalent measures are adopted, or, in exceptional circumstances in which such measures cannot be applied, the SIRO must agree this action with the Accounting Officer and notify Cabinet Office.

III.13. Wherever possible, protected personal data should be held and accessed on paper or ICT systems on secure premises (see other documents within the MPS), protected as above. This means Departments should avoid use of removable media (including laptops, removable discs, CDs, USB memory sticks, PDAs and media card formats) for storage or access to such data where possible. Where this is not possible, all Departments should work to the following hierarchy, recording the reasons why a particular approach has been adopted in a particular case or a particular business area:

13.1 the best option is to hold and access data on ICT systems on secure premises;

13.2 second best is secure remote access, so that data can be viewed or amended without being permanently stored on the remote computer. This is possible at PROTECT level over the internet using products meeting the FIPS 140-2 standard or equivalent, or using a smaller

set of products at RESTRICTED level. The National Technical Authority for Information Assurance, CESG, provides advice on suitable products and how to use them;

13.3 third best is secured transfer of information to a remote computer on a secure site on which it will be permanently stored. Both the data at rest and the link should be protected at least to the FIPS 140-2 standard or equivalent, using approved products as above. Protectively marked information must not be stored on privately owned computers unless they are protected in this way;

13.4 in all cases, the remote computer should be password protected, configured so that its functionality is minimised to its intended business use only, and have up to date software patches and anti-virus software.

III.14. Where it is not possible to avoid the use of removable media, all Departments should apply <u>all</u> of the following conditions:

14.1 the information transferred to the removable media should be the minimum necessary to achieve the business purpose, both in terms of the numbers of people covered by the information and the scope of information held. Where possible, only anonymised information should be held;

14.2 the removable media should be encrypted to a standard of at least FIPS 140-2 or equivalent in addition to being protected by a authentication mechanism, such as a password;

14.3 user rights to transfer data to removable media should be carefully considered and strictly limited to ensure that this is only provided where absolutely necessary for business purposes and subject to monitoring by managers and the information asset owner; and

14.4 the individual responsible for the removable media should handle it – themselves or if they entrust it to others – as if it were the equivalent of a large amount of their own cash.

III.15. There are some exceptional situations in which the second condition of encryption cannot be applied consistent with business continuity and disaster recovery. For example, full system back-up tapes must contain all the relevant data and Departments may judge that encrypted data cannot be recovered with sufficient speed or certainty in the event of a disaster. Such unprotected data include some of the most valuable assets owned by a Department, and should be treated accordingly, being recorded, moved, stored and monitored with strong controls – equivalent to handling arrangements for very large amounts of public money in cash. There are also specific situations in which Departments hold removable media that they cannot encrypt for legal reasons, such as when such material is collected in evidence for a legal proceeding. In those situations, the legal obligation prevails.

III.16. All material that has been used for protected data should be subject to controlled disposal. All Departments must:

16.1 destroy paper records containing protected personal data by incineration, pulping or shredding so that reconstruction is unlikely; and

16.2 dispose of electronic media that have been used for protected personal data through secure destruction, overwriting, erasure or degaussing for re-use.

III.17. Decisions on handling on the issues in paragraphs 13 – 16 should be approved in writing by the relevant information asset owner. In preparing for the annual assessment of information risk, all Departments must:

17.1 review compliance with the matrix at B or equivalent measures and any SIRO decision to take other action agreed with the Accounting Officer;

17.2 review and test documentation relating to decisions made relating to paragraphs 13 – 16;

17.3 inspect a sample of the activities of those individuals with rights to transfer protected personal data to removable media, to ensure that there is still a business case for them to have those rights;

17.4 inspect a sample of those individuals who have left roles with access to protected personal data, to ensure that access rights have been removed;

17.5 inspect a sample of removable media to ensure that required safeguards are in place;

17.6 inspect unencrypted back-ups (see paragraph 15) and reconcile them with material that has been recorded;

17.7 monitor disposal channels for paper records containing protected personal data to ensure this has been properly handled; and

17.8 ask for sample electronic media to be processed as in 16.2 and testing to attempt data recovery.

III.18. All Departments whose delivery chain involves the handling of information relating to 100,000 or more identifiable individuals must engage independent experts to carry out penetration testing of their ICT systems and to make recommendations.

Minimising risk from authorised access to protectively marked information

III.19. All Departments must ensure that all data users must successfully undergo information risk awareness training on appointment and at least annually. In addition, all information asset owners must pass information management training on appointment and at least annually, and accounting officers, SIROs, and members of the audit committee must pass strategic information risk management training at least annually.

III.20. All Departments must plan their business taking into account the information risks involved in different business models as well as their benefits. Once a business model is adopted, Departments must explicitly define and document the access rights granted to protected personal data that users enjoy, and minimise access rights within the adopted model. The information asset owner must agree in writing that access rights permit the business to be transacted with an acceptable level of risk, and if not, an alternative must be identified. Access rights should be minimised in respect of each of the following:

20.1 pool of records_accessible. The default should be that any member of staff has no access to protected personal information. If access is necessary, it should be to the smallest possible sub-set of records;

20.2 numbers of records viewed. The hierarchy should be no access / ability to view only aggregated data / ability to view only anonymous records / ability to view material from single identifiable records / ability to view material from many identifiable records simultaneously;

20.3 nature of information available. The hierarchy should be responses to defined queries (e.g. does X claim free school meals) without seeing the record / view of parts of the record itself / view of the whole record; and

20.4 functionality, including searching, alteration, deletion, printing, downloading or transferring information.

III.21. All Departments must:

20.5 put in place arrangements to log activity of data users in respect of electronically held protected personal information, and for managers to check it is being properly conducted, with a particular focus on those working remotely and those with higher levels of functionality. Summary records of managers' activity must be shared with the relevant information asset owner and be available for inspection by the Information Commissioner's Office on request; and

20.6 have a forensic readiness policy to maximise their ability to preserve, analyse and use evidence from an ICT system, should it be required.

Citizen-facing work

III.22. Departments and agencies need to ensure that citizen facing services are secure, while being easy for people or their representatives to use. Where possible, the same protective measures should be taken in transacting business with individuals as when information is stored or used within Government, but Departments should set their own proportionate standards in this area so long as those standards (and possible alternatives service routes) are clearly explained.

A: Minimum scope of protected personal data

Departments must identify data they or their delivery partners hold whose release or loss could cause harm or distress to individuals. This must include as a minimum all data falling into one or both categories below.

A. Any information that links one or more identifiable living person with information about them whose release would put them at significant risk of harm or distress.

1. one or more of the pieces of information which can be used along with public domain information to identify an individual	**combined with**	**2. information about that individual whose release is likely to cause harm or distress**
Name / addresses (home or business or both) / postcode / email / telephone numbers / driving licence number / date of birth [Note that driving licence number is included in this list because it directly yields date of birth and first part of surname]		Sensitive personal data as defined by s2 of the Data protection Act, including records relating to the criminal justice system, and group membership DNA or finger prints / bank, financial or credit card details / mother's maiden name / National Insurance number / Tax, benefit or pension records / health records / employment record / school attendance or records / material relating to social services including child protection and housing

These are not exhaustive lists. Departments should determine whether other information they hold should be included in either category.

B. Any source of information about 1000 or more identifiable individuals, other than information sourced from the public domain.

This could be a database with 1000 or more entries containing facts mentioned in box 1, or an electronic folder or drive containing 1000 or more records about individuals. Again, this is a minimum standard. Information on smaller numbers of individuals may warrant protection because of the nature of the individuals, nature or source of the information, or extent of information.

B: “Suffolk Matrix” – external access by impact / e-GIF level

Business Impact Level / “Protective Marking”	Types of data/ system included in category	e-Gif/CSIA		Network	External Access			
		Registration Level	Authentication Levels		Gov PC To WWW	WWW “café”	“PED”	Home Gov PC LAN
					WIFI	3G Data Card	Blue Tooth	Bootable USB
IL4 Confidential	Violent & Sex offenders Witness Protection	Level Three Full ID verification with appropriate vetting and need to know measures	Physical / personal / procedural protection with appropriate technical authentication mechanisms such as User Name + Password or Biometric / Certificate / Token	x.GSi xCJX	Y[1]	N	N	Y[2]
					N	N	N	Y[3]
IL3 Restricted “NHS Confidential”	Health record ContactPoint Crime Record/PNC	Level Two Cross checked ID verification with appropriate vetting and need to know measures	User Name Password / Biometric Digital Certificate	N3 GSi CJX	Y	N	Y[4]	Y[5]
					Y[6]	Y[7]	N	Y[8]
IL2 Protect	General citizen data Finance Systems	Level One Basic ID verification	User Name Password & best commercial practice	GCSx Best Commercial	Y	N	Y	Y
					Y	Y	Y[9]	Y
IL1/IL0	Google search BBC News	anonymous	No authentication required	Any	Y	Y	Y	Y

Arrangements for material at higher protective markings are dealt with separately.

[1] Via “Thin Client Internet Browse-down”
[2] Via hard-wired Government issue secure laptop (RAS)
[3] Requires a strong business case and CESG advice.
[4] Via CESG approved product such as Blackberry, Ref: CESG Procedures for Blackberry Administrators and CESG Security Procedures for Blackberry Users
[5] Via CESG-approved VPN or validated Manual T or Manual V solutions.
[6] Implementations must be compliant with CESG Manual Y
[7] Via Government issue secure laptop with software encryption (RAS)
[8] Using software-based cryptography
[9] Requires a strong business case and CESG advice