Public Services and Government

The Scottish Government

Social Research:
Data Security Review

r social research

SOCIAL RESEARCH: DATA SECURITY REVIEW

Paul Kelly and Robert Mackenzie
Scott-Moncrieff

Scottish Government Social Research
2009

This report is available on the Scottish Government Social Research website only www.scotland.gov.uk/socialresearch.

The views expressed in this report are those of the researcher and do not necessarily represent those of the Scottish Government or Scottish Ministers.

Table of Contents

1 EXECUTIVE SUMMARY

In July 2008 the Scottish Government commissioned Scott Moncrieff to review the data security procedures within eight research contractors who had regularly been commissioned to carry out social research on behalf of the Scottish Government.

1.1 The review identified that, in the main, research contractors had good procedures and processes in place to ensure compliance with data security principles. This appeared to be embedded within the sector and the existence of the ISO20252 (Market Research Standard) and guidance from the Market Research Society serves to assist in this respect. There was also a high level of awareness of the requirements of the Data Protection Act 1998 and the need for practices and processes to comply with this.

1.2 The two key issues to arise from the review were:

- There was a general absence of encryption of mobile devices which could potentially store data of a personal nature. This includes laptops (or equivalent devices) and USB memory sticks. In addition, there were no technical security controls in place to prevent the use of unencrypted USB devices on contractors' laptops and PCs. This is a potentially significant risk exposure for both research contractors and the Scottish Government as there is scope for unauthorised access to data of a personal nature in the event of the loss or theft of such devices.

- There is a need for greater clarity regarding retention and deletion of research data. A common theme from the review was reluctance on the part of contractors to delete/destroy data collected and analysed as part of the project. This reluctance was based on the fear that they may be asked to re-perform some aspects of data analysis following completion of the project. This was compounded by the absence of clear guidance from the Scottish Government clearly identifying the period for which the data should be retained. One of the eight principles of the Data Protection Act 1998 is that personal data should "not be kept for longer than is necessary". In the absence of clear guidance, it could be easily argued that the data should be permanently deleted once the final report has been published.

1.3 The Scottish Government should now consider initiating a program of actions to ensure that they, and all research contractors, implement policies and procedures which are capable of satisfying the recommendations detailed in this report.

2 INTRODUCTION

Background

2.1 Recent lapses in data security by public sector bodies and contractors has led to the loss of confidential and personal information. This has led to embarrassment for the Government and a loss of public trust.

2.2 In the financial year 2007-2008 the Scottish Government spent £7.4 million on Social research. The primary purpose of this research was to provide evidence to inform policy development and evaluate policy initiatives.

2.3 A large variety of quantitative and qualitative research is commissioned by the Scottish Government under the heading of Social research. Personal and confidential information is often collected by research contractors when exploring the attitudes, behaviour, beliefs and knowledge of the Scottish population. Details on the range of research commissioned by the Scottish Government can be found at:

http://www.scotland.gov.uk/Topics/Research/Research

2.4 The Scottish Government commissions a large number of contractors to undertake social research including academics, independent consultants, specialist research contractors and large national and international social and market research providers.

2.5 Contractors commissioned by the Scottish Government collect a wide range of personal information from members of the public. On occasion the Scottish Government may share personal information it holds centrally with research contractors to assist in the development of sampling frames and analysis. It is important that the necessary precautions are in place to ensure that this information remains confidential.

Aims and Objectives

2.6 The aim of this review was to investigate data security procedures amongst research contractors undertaking social research for the Scottish Government. The review explored the extent to which contractors are successfully complying with the provisions of the Data Protection Act 1998. A key aspect of the review was to explore the extent to which research contractors are complying with the Scottish Government terms and conditions in relation to the Data Protection Act 1998.

2.7 More specifically, the review considered the following issues:

- Are the automated systems used by contractors, protected by a level of security appropriate to the data held (e.g. firewalls or anti-virus protection on all PCs)?

- Are technical measures in place to restrict access to systems holding personal data (e.g. passwords)?
- Can USB ports be locked?
- Are technical measures in place to secure data during transit (e.g. to subcontractors and interviewers)?
- How is the data stored by sub-contractors and interviewers – is it adequate and appropriate?
- Are the premises on which the data is held secure?
- Is access to the premises restricted?
- If the data is held on non-automated systems e.g. paper files, discs, microfilm, microfiche, is access still restricted or secure?
- Are copies of printouts, obsolete back-up tapes etc disposed of securely?
- How are computer hard drives disposed of?
- Is there an auditable data retention and destruction policy?
- How effectively is information deleted / archived?
- Are staff trained and made aware of their responsibilities to safeguard the personal data? How seriously do staff take this responsibility?

2.8 This report puts forward recommendations to both the Scottish Government, as a commissioner of research, and research contractors, setting out how data security can be improved.

Approach

2.9 This review considered the procedures within eight research contractors who have regularly conducted work on behalf of the Office of the Chief Researcher (OCR) of the Scottish Government. The eight contractors varied in size and scale and, for the purposes of this report, have been split into two groups; large and small. Each group comprised four social research contractors.

2.10 The definition of each group of contractors is as follows:

- Large Contractors – Contractor has multiple office locations and has in excess of 100 staff in total.

- Small Contractors – Contractor has single office and less than 100 staff in total[1].

2.11 To ensure consistency of results, the review was focused around ISO27001, the international security standard. A questionnaire based around ISO27002, which provides best practice methods of implementing ISO27001, was developed and used for all research contractors visited. As well as being an internationally recognised standard, one of the key benefits of applying ISO27002 as the benchmark for conducting the review was that it is scalable to all contractors.

2.12 The review included visits to each of the eight contractors and meetings were held with key personnel (Information Security Officers, IT Managers, Research Consultants) who were involved in both day to day and strategic aspects of data security procedures. The review also included visits to the locations in which research data is physically held.

[1] The review included a consortium research centre whose main office was based within a major Scottish University. Under the definition used in this review the centre was classified as a small contractor.

3 RESULTS OF REVIEW

3.1 The report has been structured around each of the key areas of ISO27002, with the exception of business continuity planning and information systems acquisition, development and maintenance which were not specified as a requirement of the review.

3.2 The structure used for the questionnaire and evaluation process, and subsequently as the headings in this report, varies slightly from those used in ISO27002. This variation is based on experience of how organisations practically implement information security. However, for reference, the mapping of the report's structure to the headings used in the ISO27002 standard has been provided in the table below:

Report areas	**Mapping to ISO27002**
Security Policy	Security Policy
Security Organisation	Organisation of Information Security
Risk Assessment and Asset Management	Asset Management
Staff Education	Human Resources Security
Incident Reporting	Information Security Incident Management
Integrity of Installed Software Environment	Communications and Operations Management
Compliance with Security Requirements	Compliance
Physical and Environmental Security	Physical and Environmental Security
Network and Data Management	Access Control

Security Policy

Security Policy

3.3 A security policy is evidence of an organisation's attitude and approach to data security. The review sought to identify that not only was there a security policy in place but that there was a structured process to the development of this which involved engagement with business users.

3.4 The review identified that all of the large contractors had an information security policy. The policies themselves varied in size. Some were two pages long with others being as large as 50 pages. The shorter policy documents were supplemented with specific policies e.g. remote access. The differing approaches are both valid. However, it is generally accepted that the use of a high level, over-arching information security policy supplemented with detailed supporting policies is the most effective means of maintaining an organisation's information security policy.

3.5 Notwithstanding the variance in size and approach taken with the information security policies, the review concluded that all large contractors were able to demonstrate that the policies were in alignment with the requirements of ISO27001.

3.6 Smaller contractors did not apply quite as formal a structure. However, in virtually all of the contractors, there was some semblance of this in place. One contractor provided staff with a Data Protection Policy and guidance at induction, whereas two had a Code of Conduct/Practice that contractors felt provided appropriate guidance to staff. One relied on the policy of a larger organisation with whom they are affiliated.

3.7 In the latter case, the level of knowledge and awareness of the policy amongst staff was low. It was apparent the contractor was not involved in influencing the development to confirm that it was relevant to them. This was consistent with the overall approach to training and awareness within the contractor. Overall, there was a lack of awareness of its existence and how it applied to them.

3.8 The review noted that policy in place within smaller contractors was typically closely aligned with the process requirements of the Data Protection Act 1998 but did not necessarily consider the technical security requirements.

Recommendation for Contractors

RC1 It is recommended that appropriate processes are put in place within smaller contractors for the ongoing promotion of their security policies and raising awareness of the need for compliance. Contractors' professional bodies should be encouraged to take the lead in developing standard policies that reflect the level of best practice expected in the industry and which smaller contractors could adopt and amend, as required.

RC2 Where contractors rely on the policies of a parent or affiliated organisation, they should ensure that they are involved in the policy development process or ensure that they review the relevance of the policy to them, revise it as appropriate and promote this to their staff.

Recommendation for Scottish Government

SG1 It would be impractical to stipulate that all smaller contractors should be required to develop their own bespoke information security policy. It is, therefore, recommended that the Government consider updating their contracts to require that all contractors agree to abide by the Scottish Government's information security policies.

SG2 It may also be useful for the Government to make information security compliance part of the assessment criteria of research specifications. This would detail key information security assurance requirements and how each contractor complies with those requirements.

3.9 While the review recognised that most of the contractors, large and small, had issued policies to staff or made them available via their intranet, there was no process to confirm that staff had understood the contents of the policy. This is a vital element from both employees' and employers' perspective as it demonstrates that the policy is in existence to educate staff and contractors rather than just to "tick a box". It also provides employers with the capability to take disciplinary action should the policy be breached.

Recommendation for Contractors

RC3 It is recommended contractors implement formal mechanisms through which they can gain assurance that staff have received, read and, importantly, understood the contents of the relevant information security policies. Some examples of how this could be achieved are detailed in Annex 1.

Security Organisation

3.10 Effective data security is often directly linked to corporate culture. To be truly effective, there needs to be a positive data security culture within an organisation, supported by senior management.

Management support of information security

3.11 All of the larger contractors visited were able to demonstrate a positive attitude towards data security. It was typically the case that there was a formal structure within each contractor that ensured data security governance formed part of the overall corporate governance framework. The membership of these groups included senior, often executive management from across the contractor. Within the four large contractors it was identified that the frequency of meetings of groups was generally monthly or quarterly.

3.12 In addition, there was evidence of data security governance cascading into either low-level or departmental/functional management arrangements.

3.13 It was evident within each of the larger research contractors that there was an individual or team with responsibility for data security. It was also encouraging to note that the lead data security person in each contractor had a direct reporting line to a member of executive management.

3.14 As may be expected, the smaller research contractors did not have such formal structures in place.

3.15 The review did not find any evidence, documented or anecdotal, to suggest that there was a process in place within any of the smaller contractors to promote data security on an ongoing basis.

Recommendation for Contractors

RC4 It is recommended smaller contractors ensure that processes are put in place to demonstrate senior management support of good information security practices. This could be in the form of newsletters, email reminders, internal workshops/seminars or a regular agenda item on internal meetings.

Ownership of systems and data

3.16 A key element of data management is ensuring that there is ownership of all data within the contractor. This should assist in ensuring that there are appropriate security measures and processes in place so that the confidentiality, integrity and availability of the data is maintained.

3.17 The review identified that only two of the larger contractors had formally assigned ownership. System owners were clearly defined as were the owners of the data within those systems.

Recommendation for Contractors

RC5 It is recommended contractors ensure that all systems and data have clearly defined owners who are capable of ensuring that appropriate mechanisms are in place to securely manage and control data.

Third party agreements

3.18 The review noted that, for a number of contractors, although third party contracts/non-disclosure/confidentiality agreements were in place and in use, the third parties were not asked to formally document that they agreed to abide by the contractor's information security policy.

3.19 Moreover, it was noted that there was no consistency in the content of third party agreements. All included the need for confidentiality, however, the review did not find any which placed specific requirements on the third party to ensure their compliance with the Data Protection Act 1998. Neither were there any specific requirements in respect of the way in which they should store the data or the period for which the research data should be retained.

Recommendation for Contractors

RC6 It is recommended third party agreements are updated to incorporate specific references for third parties to comply with the requirements of the Data Protection Act 1998. This should also include examples, at least, of the expected measures to be put in place for the secure maintenance of data and processes for its secure destruction.

Recommendation for Scottish Government

SG3 It is recommended consideration be given to drafting a template third party agreement which details the minimum standards the Scottish Government expects contractors to apply when engaging third parties to conduct any aspect of social research work. Consideration should be given to incorporating a requirement within research specifications that sub-contractors formally state their compliance with Section 11 of the Scottish Government's terms and conditions.

Risk Assessment and Asset Management

Risk assessment processes

3.20 The review noted that the majority of the large contractors, with one exception, had formal risk assessment procedures in place. This ensures that there is adequate assessment of data security risks within the contractor prior to implementation of new technology or processes; e.g. the risks of the use of Blackberry devices or extending the use of remote access to the network for employees.

3.21 One of the key areas of differentiation between the four larger contractors was the classification of information. The process of classification of information assets identifies, through a security marking process, the level of authority required before access can be gained to specific information. In the UK, the Government Protective Marking Scheme recommends the following classifications:

- Not protectively marked;
- Restricted;
- Confidential;
- Secret; and
- Top Secret

3.22 It was no coincidence that the two contractors who have made greatest progress towards ISO27001 compliance were those who were actively applying an information classification scheme. The review also noted that one of the other larger contractors which had an information classification scheme was unable to provide assurance that it was applied as part of day to day practice within the contractor.

3.23 In both contractors who were actively applying an information classification scheme, it was aligned with their information asset register. An information asset register details the information held by the contractor including databases, old sets of files, recent electronic files, collections of statistics, research data etc.

3.24 Both these contractors were able to demonstrate that all information processed/held was listed along with its classification and, importantly, who

within the contractor, whether a team or individual, was the recognised owner of that information.

3.25 None of the smaller contractors visited during the review had a formal risk assessment process or information classification scheme.

Recommendation for Contractors

RC7 It is recommended all contractors consider the development of an information classification scheme. This should detail the processes through which contractor employees gain access to personal and confidential data. This will also assist in determining network access privileges.

This should be supplemented by an information asset register which details the information held by the contractor, who owns this data and its security classification. This should assist contractors in ensuring that access to information is maintained on a "need-to-have/need-to-know" basis.

Transmission of data

3.26 One of the key areas of focus of the review related to encryption in terms of both the transmission and storage of data.

3.27 The majority of contractors visited appeared to be aware of the risks involved in the transmission of personal data. In all contractors, it was commented that transmission of personal data was actively discouraged unless absolutely necessary.

3.28 For all contractors, it was noted that technology was available for the secure transmission of files. This varied from specialist encryption tools within email systems, encrypted zip files and use of secure technologies to exchange data files over the internet e.g. Secure FTP (File Transfer Protocol). The review found that all of the technical solutions deployed used robust encryption methods.

3.29 Whilst the facility was in place to use these tools, it was evident that their use was at the individual's discretion. Therefore, there is a risk of data leakage from contractors as they are unable to provide assurance that all data that should be securely transmitted is sent securely, using the relevant tools.

Recommendation for Contractors

RC8 It is recommended that contractors improve controls within their organisation so that they can gain assurance that all data transmitted is appropriately secured using the technology available. See Annex 2 for further information.

Recommendation for Scottish Government

SG4 It is recommended that the Scottish Government include within their terms and conditions of contract that there is appropriate encryption of all personal data transmitted by email or other storage media.

Asset management and security

3.30 The review noted that all contractors maintained an inventory of IT hardware assets. However, the review identified that this did not extend to USB memory sticks. The review identified that there was a general absence of controls which allowed contractors to monitor USB memory sticks in use, or to confirm whether any had been lost or stolen.

3.31 Almost certainly the area of greatest concern to arise during the review was that no contractor was using encrypted USB memory sticks. This was surprising given the volume of media publicity relating to data loss resulting from misplaced or stolen USB memory sticks. All contractors had memory sticks in issue. Whilst all contractors said that staff had been informed that personal data should not be held on such devices, technical security controls were not in place to prevent this.

3.32 A good example of the potential weaknesses of using soft policy, as opposed to technical controls, in managing and controlling the use of USB memory sticks was highlighted with the practice of one contractor. This contractor stated that their staff were instructed that if sensitive material was to be placed on a USB memory stick it should be encrypted beforehand. As stated above, there are no detective controls in place within contractor organisations that ensure staff follow this guidance. Consequently, there is a risk that unencrypted information could be transferred to USB memory sticks. If lost, this could result in the data being compromised and lead to significant reputational damage to both the contractor and the Scottish Government.

Recommendation for Contractors

RC9 It is recommended that all contractors ensure that they only use encrypted USB devices.

RC10 It is also recommended that all contractors maintain an inventory of all USB devices.

Recommendation for Scottish Government

SG5 It is recommended that the Scottish Government mandate that research contractors must use encrypted USB devices when conducting social research work.

Restriction on USB devices

3.33 The review identified that no contractors had technical security controls in place to prevent the use of USB devices. This means that devices such as memory sticks and other devices that have flash memory or hard disk memory; e.g. iPods, mobile phones, portable/external hard disk drives can readily be connected to a PC or laptop without any technical security measures being in place to block this. This exposes both the Scottish Government and research contractors to the risk of data theft. The storage capability of many of the devices described above means that it is possible for the entire server of a small contractor to be copied to an external device without being detected.

3.34 The review did note that some of the larger contractors are investigating the deployment of solutions that will allow improved controls over the connection of USB devices to PCs or laptops.

Recommendation for Contractors

RC11 It is recommended contractors ensure that they investigate the controls they could put in place to prevent the connection of unauthorised and unencrypted USB devices to PCs or laptops. This should consider the use of Windows Group Policy Objects functionality and, potentially, products available on the market.

Recommendation for Scottish Government

SG6 It is recommended the Scottish Government mandate that contractors must be able to demonstrate that they are using controlled and encrypted USB memory sticks whilst undertaking any social research work. Alternatively, as an interim solution, the Scottish Government should obtain a formal undertaking that USB memory sticks will not be used for Scottish Government social research projects.

Staff Education

3.35 As stated previously in this report, the past year has seen unprecedented media publicity in respect of data security e.g. HMRC data disks, loss of MoD laptops. This has significantly increased the profile of data security and its importance in maintaining the reputation of an organisation. Recent cases have highlighted that data loss is typically a result of failure of people and process. Therefore, the ongoing training and development of staff is a critical aspect of ensuring good data security practices. This training can be delivered in different formats; e.g. seminars, computer based training etc.

Training and awareness

3.36 Generally speaking, the review identified that larger contractors had delivered some formal training to staff to make them aware of good data security practices. However, the review noted that this training was generally found to relate to the introduction of ISO27001 accreditation/ compliance processes or revised information security policies.

3.37 The review noted, however, that there was a lack of clarity within larger contractors with respect to the ongoing provision of data security training for staff. The review identified that contractors were assessing the mechanisms that they could use for delivery of ongoing training rather than there being formal training plans in place.

3.38 The review identified that one of the larger contractors had not conducted any recent data security training for staff other than that delivered as part of induction. The review recognises, however, that the contractor was in the early stages of a procurement exercise to select a supplier to deliver data security training.

3.39 None of the smaller contractors were able to demonstrate evidence of formal arrangements as a means of ensuring that their staff were provided with training on data security issues.

3.40 The review noted that, within smaller contractors, data protection/security issues formed part of the induction process. However, there was no evidence of a process to provide ongoing data security training and awareness. Several smaller contractors stated that a common sense approach was advocated to staff. This could be regarded as a high-risk practice as there is no consistent approach to the secure handling of data which staff can regard as good practice. This could also result in the development of different and possibly conflicting working practices across a contractor.

3.41 The review did identify that all contractors considered a breach of data security by an employee to be a disciplinary issue.

Recommendation for Contractors

RC12 It is recommended all contractors ensure that they maintain and deliver a programme of ongoing information security training and awareness for staff so that they are aware of potential risks to the security of data. The mechanisms that could be used to achieve this are varied and could include formal training sessions (internally or externally provided), use of computer-based training, regular email alerts, newsletters, intranet, flyers attached to payslips etc.

Consideration should be given to the role professional associations such as the Social Research Association (SRA) and the Market Research Society (MRS) could play in the provision of training to contractors and their staff.

Incident Reporting

3.42 In today's data security climate, it is critical that there are appropriate systems and processes in place within an organisation to ensure that any actual or suspected data security incidents are identified, reported and investigated with appropriate/necessary actions taken to prevent their recurrence.

3.43 As previously mentioned, the majority of large contractors had formal governance structures in place through which data security incidents were reported.

3.44 The one common theme noted in the review was that there was no formal explanation or definition of what actually constitutes an incident. Therefore, there is a risk that staff may not be fully aware of when an incident should be reported

3.45 The review noted that smaller contractors did not have any formal procedures in place for dealing with information security incidents. There was a reliance on staff to highlight any issues and report them to the appropriate personnel within the organisation. The absence of a formal approach means that the review could not establish that incidents would be subject to formal investigation and actions taken to prevent their recurrence.

3.46 The Information Commissioner has issued guidance relating to the reporting of serious breaches of data security and the processes for dealing with security breaches. These can be found at:

http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/breach_reporting.pdf

http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/guidance_on_data_security_breach_management.pdf

Recommendation for Contractors

RC13 It is recommend all contractors, as part of their policies and training programmes, provide guidance to staff on what should be regarded as an information security incident. This should assist in highlighting the importance of information security and clarifying responsibilities for processing and holding data.

RC14 It is also recommended that contractors ensure they develop formal procedures for the management of information security incidents. This should ensure compliance with the guidance from the Information Commissioner identified above in 3.46.

RC15 It is also recommended that contractors make the Scottish Government aware of any data security incidents relating to social research projects.

Recommendation for Scottish Government

SG7 It is recommended, potentially as part of the assessment criteria, that the Scottish Government require contractors to confirm that they will comply with the standards and guidance issued by the Information Commissioner for the management and reporting of data security breaches.

SG8 It is recommended the Scottish Government amend their terms and conditions of contract to require that they must be notified immediately by contractors of any data security incidents relating to social research projects.

Integrity of Installed Software Environment

3.47 It is essential that there are appropriate technical security controls in place to protect an organisation's data from external threat such as viruses, malicious software and denial of service attacks (a concerted attempt to make computer resources unavailable to intended users).

3.48 The review noted that all research contractors had appropriate anti-virus solutions and firewalls in place. This is consistent with practice in other sectors. The review identified that virtually every organisation has taken appropriate steps to protect their networks from external threats by the implementation and professional management of anti-virus and firewall solutions. The larger contractors managed firewalls using their own in-house personnel whereas smaller contractors outsourced this to a professional IT services company.

3.49 The one area where the review noted a potential weakness related to the practices of one of the smaller research contractors. Their staff were allowed to use their home PCs to create a remote connection to the corporate network. This was achieved through the use of a secure virtual private network (VPN) connection. There was no assurance gained by the contractor that staff with this facility have appropriate and up to date anti-virus and firewall software. Therefore, this increases the risk of virus infection on the corporate network and corruption of data. It also increases the risk of the security of the corporate network being compromised, particularly if unsecured wireless broadband is used by the member of staff.

Recommendation for Contractors

RC16 It is recommended that assurance is obtained that all remote/home workers have appropriate technical security controls in place to protect the network from virus infection or unauthorised access.

RC17 As a minimum, this should include personal anti-virus and firewalls solutions. These should be configured to update on a regular (daily) basis so that the PC/laptop is protected from the latest known viruses and vulnerabilities. Contractors should request their IT services provider to recommend the most appropriate solution and provide assistance with its installation and configuration.

Compliance with Security Requirements

3.50 A core part of compliance with good data security practice is being able to demonstrate the legislation that applies to the organisation and identify those responsible for ensuring compliance with each piece of legislation.

Awareness of legislation

3.51 The awareness of the need to comply with the Data Protection Act 1998 was extremely high and appeared to be embedded within the culture of each contractor. This was evident as part of the processes in collecting data via face to face interviews i.e. Computer Assisted Personal Interviews (CAPI) or through completion of forms whether in person or through postal submissions. The review also noted that the processes for holding and subsequently analysing data appeared to be similarly robust.

3.52 However, with one exception, research contractors had not formally compiled a list of the legislation that impacts on the manner in which they conduct business.

Recommendation for Contractors

RC18 It is recommend contractors identify all legislation that impacts on their business, particularly where it may affect processes that impact on compliance with information security related practices. A named individual within the contractor should be assigned responsibility for ensuring that there is compliance with the requirements of the legislation. Contractors' professional bodies should be encouraged to participate in the development of services which could assist contractors in addressing this issue.

Data collection

3.53 The review identified that, when conducting CAPI interviews, laptop-equivalent devices such as tablet PCs are used. When completing the questionnaire, a file is created with the responses provided. The review identified that the data files are retained on the device until all of the questionnaires are complete.

3.54 In discussing this process, the review noted that not all laptops used for this purpose are encrypted. Of the four larger contractors, laptop encryption was as follows:

- One had all of their laptops encrypted;
- One did not have any encryption;
- One had approximately one third of their laptops encrypted and were in the process of encrypting all laptops; and
- One did not have all of their laptops encrypted but stated that when conducting work for the Government encrypted devices were used.

3.55 The review identified that none of the smaller contractors had encrypted laptops in use. Therefore, there is a risk that in the event of loss or theft of a CAPI laptop, access could be gained to any personal data on it, some of which may be sensitive.

Recommendation for Contractors

RC19 It is recommended contractors ensure all laptops used for the collection, processing and storage of data have whole disk encryption to prevent leakage of data to unauthorised parties.

The costs of implementing whole disk encryption will vary depending on the solution implemented. However, it is broadly estimated that whole disk encryption can be achieved at a cost of between £50-60 per PC/laptop.

Recommendation for Scottish Government

SG9 It is recommended the Scottish Government mandate that all laptops and all other storage media used for the purposes of their social research projects have whole disk encryption. Contractors should be required to formally confirm their compliance with this requirement, potentially within the assessment criteria suggested above.

SG10 It is recommended the Scottish Government make reference to the NHS Scotland Mobile Data Protection Standard as a means of providing guidance to contractors on solutions that could be deployed. The standard can be found at:

http://www.ehealth.scot.nhs.uk/wp-content/documents/mobile-data-protection-standard-pdf3.pdf

3.56 The review identified that some data is also gathered using manually completed questionnaires, although the consensus was that these are diminishing and will only be used for small research projects.

3.57 Depending on the approach, questionnaires will either be sent to respondents within the original sample who are asked to complete this and return it to the research contractor or it will be completed during an interview by a member of the field staff of the research contractor. For some of the contractors who used questionnaires for face-to-face interviews, personal information was

recorded on the front cover of the questionnaire. In one contractor, the review noted that the questionnaire contained two cover pages. The first cover page recorded personal data relating to the respondent (data subject) and a unique reference. The second cover page would only contain the unique reference.

3.58 The review noted that the general approach was that the field interviewers would complete the questionnaires, consolidate them in batches of 10-25 and then send these using Royal Mail, normally using Special Delivery although some used first class standard delivery. However, the review noted that the front cover page containing personal data would only be removed upon receipt at the offices of the research contractor. These would be held separately from the completed questionnaires. The reason given for holding this personal information is to allow internal quality checks to be performed i.e. to verify the respondent's participation in the research.

3.59 There is a risk that questionnaires could be lost in transit or sent to an incorrect address and personal data could be compromised.

Recommendation for Contractors

RC20 It is recommended that contractors ensure that all completed questionnaires relating to Scottish Government social research projects are submitted in a manner which ensures the responses are anonymous. Contractors should use secure courier companies for the transportation of questionnaires. They should also ensure that all person-identifiable information is removed and sent separately from the questionnaire.

Deletion of data

3.60 The review found that there were internal policies/procedures within all contractors regarding the process to be followed for deleting source/sample data on completion of a research project. Whilst the review acknowledges the existence of this, the review identified there was no defined process in place within contractor organisations to confirm that the source/sample data files were deleted.

3.61 One of the most common issues the review identified was the general reluctance to delete data relating to research projects. At virtually every contractor visited, a comment was made that researchers did not want to delete the data for fear that they may be asked to refer back to it in the future. This was acutely demonstrated at one of the smaller contractors who had a sample file containing personal data which dated back to early 2000. One of the eight principles of the Data Protection Act 1998 specifically states that personal data should *"not be kept for longer than is necessary".*

3.62 The review identified through discussions with contractors, that they were not always clear on the period for which the data needs to be retained. The review identified that the data retention period is explicitly specified in contracts.

3.63 The review identified an added complication in this respect with the retention of back-up tapes by contractors. Many of the contractors hold monthly and annual back-up tapes indefinitely. There is a high risk that these tapes may hold information of a personal nature that is no longer required to be held. There is no check performed on the contents of these tapes to confirm whether any personal data is held on these.

3.64 In addition, the review found that the contractors did not have formal retention and destruction policies to support the processes for storage and deletion of data.

Recommendation for Contractors

RC21 It is recommended that contractors:

- Develop formal internal processes to confirm that all data that no longer needs to be held for the purposes of the research project is deleted timeously.
- Ensure all data held that may be of a personal nature is deleted as soon as possible after completion of the project in compliance with the requirements of the Data Protection Act 1998, unless there is specific contractual provisions to state otherwise.
- Develop a formal information retention and destruction policy so that there is clarity across the contracting organisation over the process for managing and controlling information held.

RC22 It is recommended that contractors ensure all back-up tapes are checked to confirm that there is no personal data held that is no longer required to be held.

Recommendation for Scottish Government

SG11 It is recommended that when awarding contracts for conducting social research projects, the Scottish Government:

- More explicitly define the time period they wish to retain sample data for. This will provide clarity over data retention periods and ensure that all parties are aware of their responsibilities for complying with the Data Protection Act.
- Request contractors to declare that they have deleted all personal data in accordance with contracted requirements.
- Make it a formal requirement for contractors to state their policy on retention and destruction and that this forms part of the assessment criteria of research specifications.

Destruction of storage media

3.65 One of the key areas of the review was the process for destroying storage media. In the main, researchers were using external companies for the destruction of PC and laptop hard disk drives. Some of the contractors, both small and large, stated that they securely destroy the disks themselves using appropriate means to do so e.g. use of secure destruction companies. The review identified that one of the smaller contractors stated that they will occasionally sell an old PC or laptop to a member of staff. Whenever they do this, they re-format the hard drive of the PC/laptop and re-install the operating system software. Unfortunately, re-formatting a hard disk drive does not permanently delete data files from the disk and forensic tools can be used to potentially recover data.

3.66 The review identified that back-up tapes tend not to be destroyed and were instead retained indefinitely. Where they were destroyed, the review found that this was done in a secure manner.

3.67 One of the issues identified by the review related to other storage media such as DVDs and CDs. These could hold both the sample data for a research project or be used internally to store data. The review identified that no research contractor could confirm that they knew of all DVDs or CDs in use and whether they were used to hold personal data.

3.68 The review also identified that some of the larger contractors offices had shredders on each floor, that complied with DIN 3 standards and which are adequate for shredding information up to confidential classification. The review noted that contractors stated CDs and DVDs should be disposed of securely but in a number of the contractors the review could not readily identify how assurance could be gained that this was done.

3.69 A number of contractors stated that they discouraged the use of CDs or DVDs. One of the larger contractors stated that many of their PCs did not contain CD or DVD burners.

Recommendation for Contractors

RC23 It is recommended that all contractors use appropriate software or secure destruction companies to ensure the destruction of data files contained on PC or laptop hard disks. In the case of software utilities, there are several, affordable products on the market which can be used to erase disk contents to US Department of Defence standards (this is the generally accepted compliance standard).

RC24 It is also recommended contractors ensure staff are reminded of how to secure other storage media i.e. CDs and DVDs appropriately. It is also recommended that contractors ensure that there are processes in place to ensure both the safe and timeous destruction of CDs and DVDs so that the requirements of the Data Protection Act 1998 are complied with.

Audit

3.70 The review noted that some of the larger contractors had in-house internal audit functions. The review generally found that there had not been any specific assessment of IT or information security. The internal audit functions tended to be business process focused. Such audits may comment on IT and information security risks in individual areas rather than in totality. The review also noted that one of the larger contractors had an independent review conducted to assess their compliance with information security best practice.

3.71 No smaller contractors had had any audit conducted of IT or information security risks.

Recommendation for Contractors

RC25 It is recommended contractors, especially large contractors, consider conducting information and IT security reviews, at least annually, as part of their ability to gain assurance that good information security practices are in place. This could be achieved through in-house audit functions or an independent external auditor. This would provide senior management within contractors with assurance or identify gaps in compliance with security policies.

Physical and Environmental Security

3.72 It is essential for all organisations that appropriate physical and environmental security controls are in place to protect data from loss or theft. This includes core IT infrastructure devices such as servers and communications equipment as well as CDs, DVDs and back-up tapes, which may hold data relating to research projects.

Computer rooms

3.73 The review identified that all of the larger contractors visited had a dedicated facility within their offices (or at another office belonging to the contractor) where core IT infrastructure was located. All of the computer rooms had access control arrangements. The review found that some were better than others at recording individual access to the room. At two of the four larger research contractors visited, it was not formally recorded that the reviewer had accessed the room.

3.74 The review noted that for all four large contractors, computer rooms were located in close proximity to IT staff and generally remote from operational staff. None of the rooms could be readily identified as a computer room by a passer-by/layperson.

3.75 All of the computer rooms had appropriate air conditioning systems in place. Environmental monitoring systems varied between the contractors but this was, adequately, explained as risk management.

3.76 The review identified that the situation was not as well controlled within smaller contractors. The review noted at two of the smaller contractors that core IT infrastructure was not held securely. Whilst the review recognises that the smaller contractors will not have the financial or space resources, the storage arrangements could not be considered to be secure. In both cases, equipment was stored in open areas of the office, accessible to employees.

3.77 The infrastructure of one of the smaller contractors was hosted within the computer room of a secure facility belonging to an organisation with whom they are affiliated. The reviewer was satisfied that the physical security of the other smaller contractor was adequate to support secure mobile/tele-working.

Recommendation for Contractors

RC26 It is recommended smaller contractors improve the physical and environmental security of their core IT infrastructure devices. These should be maintained in a secure, temperature controlled environment to prevent accidental or malicious interference with the devices.

Office security

3.78 The review incorporated visits to the offices of all eight participating research contractors. This also included visits to the locations where research data was physically held.

3.79 The review noted that the physical security of the buildings was generally good. Almost all of the buildings had access control systems and/or a manned reception that would provide challenge to anyone wishing to enter the building. Within the buildings themselves, a number of the larger contractors had internal access control systems which restricted movement of people. The review also noted that, in the main, filing cabinets were in use and locked when left unattended.

3.80 The review identified that one of the smaller contractors did not have formal access control systems in place to prevent unauthorised access to their offices. Although there was a reception desk, at the time of the review this was not manned.

Recommendation for Contractors

RC27 It is recommended contractors ensure that there are adequate access control arrangements in place for all offices where data is processed or IT infrastructure hosting data is located. This should be sufficient to prevent unchallenged access to office areas.

Network and Data Management

User account management

3.81 The review identified that all network users have a unique user id and password. The processes for the creation, amendment and deletion of user accounts were also found to be reasonably generic. Although IT personnel were responsible for administration of the user accounts, authorisation was required from line managers to create, amend or delete these.

3.82 As is the case in many organisations, there was scope within the majority of contractors for improving the processes for managing user accounts for leavers and, aligned with that, the process for returning assets (i.e. laptops, Blackberry devices, USB memory sticks etc) for the majority of contractors. This is of higher risk in larger contractors given their larger workforce and higher staff turnover. The review noted that there is almost complete reliance placed on line managers to inform IT whenever staff submit their resignation so that the necessary processes can be put in place to remove network privileges and identify all assets to be returned.

Recommendation for Contractors

RC28 It is recommended contractors give consideration to enhancing the robustness of the leaver process to ensure that the respective IT personnel are made aware of the leaving date. This should ensure that measures can be put in place to disable user accounts and ensure that line managers can recover all IT assets provided. This should also be extended for situations of extended periods of absence i.e. sickness, maternity leave, careers breaks etc.

Password controls

3.83 The review noted that, with the exception of two of the larger contractors, there was scope for improvement of password controls.

3.84 Only two of the contractors had password complexity enabled and password length varied between 6 and 8 characters. Password complexity is the use of upper and lower case alpha characters combined with numbers and special characters (#, $ etc.). It provides an added layer of assurance regarding the security of user accounts as passwords are less likely to be compromised as a result of guessing or brute-force attack from password cracking utilities.

3.85 Of most significant concern was one small contractor whose password policy was very weak. The contractor had password settings of:

- Maximum password age = 0
- Password length = 0

3.86 This means that the user is never forced to change their password and they could have a blank password, potentially rendering any network security meaningless. This is of great concern for those users with access to data that is of a personal nature.

Recommendation for Contractors

RC29 It is recommended contractors consider implementing the following as a **minimum** standard for passwords, as recommended by the US National Security Administration for Windows 2003 servers for normal enterprises:

- Passwords remembered = 24
- Maximum password age = 42 days
- Minimum password age = 1 day
- Password length = 8
- Complexity = enabled

All of the above settings should ensure robust password security.

Recommendation for Scottish Government

SG12 It is recommended that the Scottish Government consider including the password setting identified above as the minimum standards to be applied by contractors. This could be specified as a requirement of the information security assessment criteria.

3.87 The review also noted that there was evidence of password sharing. Two smaller contractors stated that passwords were known to other people. At one contractor, the company directors were aware of staff passwords. At the other contractor, all user passwords were known to the person responsible for IT. This is a fundamental weakness and completely compromises user account security.

Recommendation for Contractors

RC30 It is recommended contractors ensure that passwords for user accounts are only known to the owner of that account so that the integrity of the accounts is not compromised.

User access to information

3.88 The review identified a mix of practice with regard to access to network folders and research data at smaller contractors. In general, access to research project folders was determined by the respective lead project officer within the contractor. However, there were inconsistencies in practice across all of the contractors in determining who should have access to the information. Good data security practice states that access to data should be on a "need-to-have/need-to-know" basis. This ensures that staff can only get access to information for which they can demonstrate a clear need.

3.89 The larger contractors tended to have a policy that restricted access to specific project folders for consultants and field staff, while all analysis staff would have access to all project folders. The justification given was that, on a

practical level, any member of the analysis team could be assigned to a project.

3.90 The review noted that in smaller contractors, access to research project folders was open to all staff regardless of their position and involvement in specific contracts.

3.91 The review did not identify any evidence of a regular process being adopted to confirm the level of access each user has to data and whether it is appropriate.

Recommendation for Contractors

RC31 It is recommended contractors consider implementing network security controls in parallel with the requirements of their information security policy so that access to information is on a "need-to-have/need-to-know" basis. This will provide assurance that access to data, which may be of a personal nature, is only available to those who actually require it.

Network vulnerability testing

3.92 Technical network vulnerability assessment is the process of gaining assurance that the network is protected from external threats.

3.93 This was an area where large contractors demonstrated good practice. All either had conducted independent penetration tests (by an external company) or had tools to allow them to self-assess the security of the perimeter of the network. There was no such process in smaller contractors.

Recommendation for Contractors

RC32 It is recommend smaller contractors undertake appropriate testing of their network perimeter, at least annually, to gain assurance that it is secure from external attack. This could potentially be conducted under the existing service contracts with external providers.

The cost of performing these tests will vary depending on the complexity of an organisation's network infrastructure. For example, an organisation with a single site and single external connection to the internet would expect to pay upwards of £3,000 whereas a large, multi-site organisation with numerous points of connection to the internet would expect costs to start at £15,000.

Conclusion

3.94 Overall, the review identified a number of areas of good practice and compliance with good information security practice across the research contractors.

3.95 The approach taken during the review has allowed an assessment to be made of both the large and small contractors' compliance with the best practice guidance defined within ISO27002 and this has been included in the table below.

Level of contractor compliance with good practice		
ISO27002 Questionnaire Area	**Large Contractors**	**Small Contractors**
Security Policy	**HIGH**	**MEDIUM**
Security Organisation	**HIGH**	**LOW**
Risk Assessment	**MEDIUM**	**LOW**
Staff Education	**MEDIUM**	**LOW**
Incident Reporting	**MEDIUM**	**MEDIUM**
Integrity of Installed Software Environment	**HIGH**	**HIGH**
Compliance with Security Requirements	**MEDIUM**	**MEDIUM**
Physical and Environmental Security	**HIGH**	**MEDIUM**
Network and Data Management	**MEDIUM**	**LOW**

3.96 This compliance level has been assessed using the follow criteria:

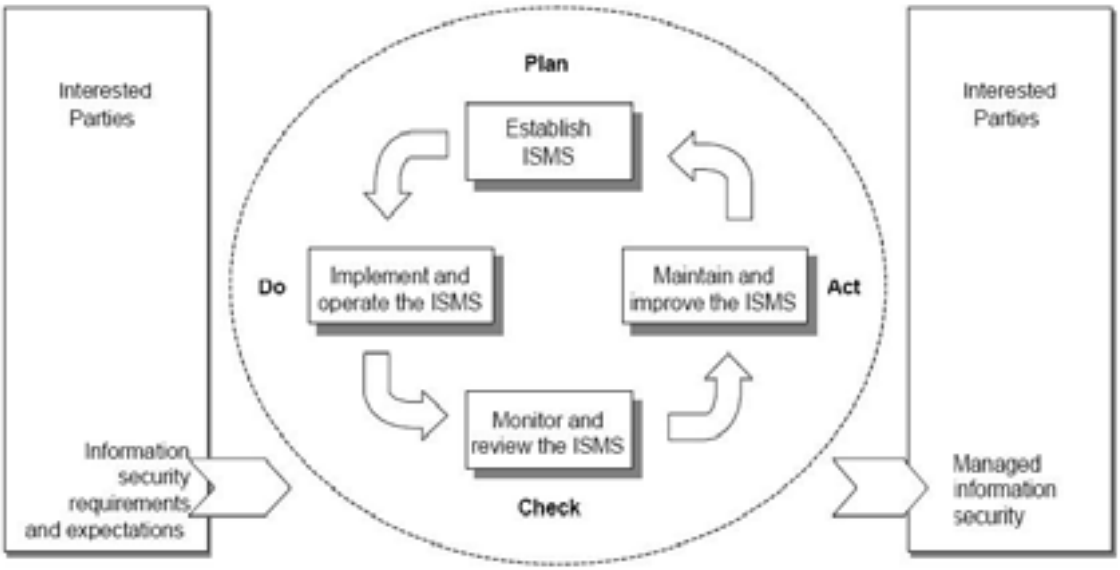
Compliance	**Description**
High	Contractor has been able to demonstrate they have adequate practices and processes in place to minimise data security risks.
Medium	Contractor requires to make minor improvement to practices and processes to minimise data security risks.
Low	Contractor requires to make improvement to practices and processes to minimise data security risks.

3.97 The review identified that, in the main, research contractors had good procedures and processes in place to ensure compliance with data security principles. This appeared to be embedded within the sector and the existence

of the ISO20252 (Market Research Standard) and guidance from the Market Research Society serves to assist in this respect. There was also a high level of awareness of the requirements of the Data Protection Act 1998 and the need for practices and processes to comply with this.

3.98 The review noted that there is scope for improvement across both large and small contractors in their information security practices. Although there are several areas where the review has noted that small contractors have demonstrated low compliance with good practice, the resources (financial and human) required to increase compliance is not significant. For example, staff education should form part of the contractor's overall training process. Similarly, management support of information security could also be achieved relatively easily through promotion of policies and emails to all staff reminding them of the importance of information security.

3.99 The review found that large contractors generally had good and well established practices in place to ensure effective information security practices. The recommendations contained in this review should form part of the ongoing development of information security management within these contractors. This is consistent with the ISO27001 standard which recommends continuous improvement as part of the development and maintenance of an information security management system, as shown in the diagram[2] below:



[2] *Source: Information Technology - Security Techniques – Information Security Management Systems – Requirements (BS ISO/IEC 27001:2005 BS7799:2-2005)* produced by BSi (British Standards Institution)

4 RECOMMENDATIONS

4.1 Detailed below are the recommendations for both research contractors and the Scottish Government. Not all of the recommendations apply to all research contractors but should provide a reminder at the very least of the practices and standards to be applied when performing social research projects.

Recommendations for Contractors

4.2 Listed below are all of the recommendations that apply to research contractors.

Security Policy

Recommendation for Contractors

RC1 It is recommended that appropriate processes are put in place within smaller contractors for the ongoing promotion of their security policies and raising awareness of the need for compliance. Contractors' professional bodies should be encouraged to take the lead in developing standard policies that reflect the level of best practice expected in the industry and which smaller contractors could adopt and amend, as required.

RC2 Where contractors rely on the policies of a parent or affiliated organisation, they should ensure that they are involved in the policy development process or ensure that they review the relevance of the policy to them, revise it as appropriate and promote this to their staff.

Recommendation for Contractors

RC3 It is recommended contractors implement formal mechanisms through which they can gain assurance that staff have received, read and, importantly, understood the contents of the relevant information security policies. Some examples of how this could be achieved are detailed in Annex 1.

Security Organisation

Recommendation for Contractors

RC4 It is recommended smaller contractors ensure that processes are put in place to demonstrate senior management support of good information security practices. This could be in the form of newsletters, email reminders, internal workshops/seminars or a regular agenda item on internal meetings.

Recommendation for Contractors

RC5 It is recommended contractors ensure that all systems and data have clearly defined owners who are capable of ensuring that appropriate mechanisms are in place to securely manage and control data.

Recommendation for Contractors

RC6 It is recommended third party agreements are updated to incorporate specific references for third parties to comply with the requirements of the Data Protection Act 1998. This should also include examples, at least, of the expected measures to be put in place for the secure maintenance of data and processes for its secure destruction.

Risk Assessment and Asset Management

Recommendation for Contractors

RC7 It is recommended all contractors consider the development of an information classification scheme. This should detail the processes through which contractor employees gain access to personal and confidential data. This will also assist in determining network access privileges.

This should be supplemented by an information asset register which details the information held by the contractor, who owns this data and its security classification. This should assist contractors in ensuring that access to information is maintained on a “need-to-have/need-to-know” basis.

Recommendation for Contractors

RC8 It is recommended that contractors improve controls within their organisation so that they can gain assurance that all data transmitted is appropriately secured using the technology available. See Annex 2 for further information.

Recommendation for Contractors

RC9 It is recommended that all contractors ensure that they only use encrypted USB devices.

RC10 It is also recommended that all contractors maintain an inventory of all USB devices.

Recommendation for Contractors

RC11 It is recommended contractors ensure that they investigate the controls they could put in place to prevent the connection of unauthorised and unencrypted USB devices to PCs or laptops. This should consider the use of Windows Group Policy Objects functionality and, potentially, products available on the market.

Staff Education

Recommendation for Contractors

RC12 It is recommended all contractors ensure that they maintain and deliver a programme of ongoing information security training and awareness for staff so that they are aware of potential risks to the security of data. The mechanisms that could be used to achieve this are varied and could include formal training sessions (internally or externally provided), use of computer-based training, regular email alerts, newsletters, intranet, flyers attached to payslips etc.

Consideration should be given to the role professional associations such as the Social Research Association (SRA) and the Market Research Society (MRS) could play in the provision of training to contractors and their staff.

Incident Reporting

Recommendation for Contractors

RC13 It is recommend all contractors, as part of their policies and training programmes, provide guidance to staff on what should be regarded as an information security incident. This should assist in highlighting the importance of information security and clarifying responsibilities for processing and holding data.

RC14 It is also recommended that contractors ensure they develop formal procedures for the management of information security incidents. This should ensure compliance with the guidance from the Information Commissioner identified above in 3.46.

RC15 It is also recommended that contractors make the Scottish Government aware of any data security incidents relating to social research projects.

Integrity of Installed Software Environment

Recommendation for Contractors

RC16 It is recommended that assurance is obtained that all remote/home workers have appropriate technical security controls in place to protect the network from virus infection or unauthorised access.

RC17 As a minimum, this should include personal anti-virus and firewalls solutions. These should be configured to update on a regular (daily) basis so that the PC/laptop is protected from the latest known viruses and vulnerabilities. Contractors should request their IT services provider to recommend the most appropriate solution and provide assistance with its installation and configuration.

Compliance with Security Requirements

Recommendation for Contractors

RC18 It is recommend contractors identify all legislation that impacts on their business, particularly where it may affect processes that impact on compliance with information security related practices. A named individual within the contractor should be assigned responsibility for ensuring that there is compliance with the requirements of the legislation. Contractors' professional bodies should be encouraged to participate in the development of services which could assist contractors in addressing this issue.

Recommendation for Contractors

RC19 It is recommended contractors ensure all laptops used for the collection, processing and storage of data have whole disk encryption to prevent leakage of data to unauthorised parties.

The costs of implementing whole disk encryption will vary depending on the solution implemented. However, it is broadly estimated that whole disk encryption can be achieved at a cost of between £50-60 per PC/laptop.

Recommendation for Contractors

RC20 It is recommended that contractors ensure that all completed questionnaires relating to Scottish Government social research projects are submitted in a manner which ensures the responses are anonymous. Contractors should use secure courier companies for the transportation of questionnaires. They should also ensure that all person-identifiable information is removed and sent separately from the questionnaire.

Recommendation for Contractors

RC21 It is recommended that contractors:

- Develop formal internal processes to confirm that all data that no longer needs to be held for the purposes of the research project is deleted timeously.
- Ensure all data held that may be of a personal nature is deleted as soon as possible after completion of the project in compliance with the requirements of the Data Protection Act 1998, unless there is specific contractual provisions to state otherwise.
- Develop a formal information retention and destruction policy so that there is clarity across the contracting organisation over the process for managing and controlling information held.

RC22 It is recommended that contractors ensure all back-up tapes are checked to confirm that there is no personal data held that is no longer required to be held.

Recommendation for Contractors

RC23 It is recommended that all contractors use appropriate software or secure destruction companies to ensure the destruction of data files contained on PC or laptop hard disks. In the case of software utilities, there are several, affordable products on the market which can be used to erase disk contents to US Department of Defence standards (this is the generally accepted compliance standard).

RC24 It is also recommended contractors ensure staff are reminded of how to secure other storage media i.e. CDs and DVDs appropriately. It is also recommended that contractors ensure that there are processes in place to ensure both the safe and timeous destruction of CDs and DVDs so that the requirements of the Data Protection Act 1998 are complied with.

Recommendation for Contractors

RC25 It is recommended contractors, especially large contractors, consider conducting information and IT security reviews, at least annually, as part of their ability to gain assurance that good information security practices are in place. This could be achieved through in-house audit functions or an independent external auditor. This would provide senior management within contractors with assurance or identify gaps in compliance with security policies.

Physical and Environmental Security

Recommendation for Contractors

RC26 It is recommended smaller contractors improve the physical and environmental security of their core IT infrastructure devices. These should be maintained in a secure, temperature controlled environment to prevent accidental or malicious interference with the devices.

Recommendation for Contractors

RC27 It is recommended contractors ensure that there are adequate access control arrangements in place for all offices where data is processed or IT infrastructure hosting data is located. This should be sufficient to prevent unchallenged access to office areas.

Network and Data Management

Recommendation for Contractors

RC28 It is recommended contractors give consideration to enhancing the robustness of the leaver process to ensure that the respective IT personnel are made aware of the leaving date. This should ensure that measures can be put in place to disable user accounts and ensure that line managers can recover all IT assets provided. This should also be extended for situations of extended periods of absence i.e. sickness, maternity leave, careers breaks etc.

Recommendation for Contractors

RC29 It is recommended contractors consider implementing the following as a **minimum** standard for passwords, as recommended by the US National Security Administration for Windows 2003 servers for normal enterprises:

- Passwords remembered = 24
- Maximum password age = 42 days
- Minimum password age = 1 day
- Password length = 8
- Complexity = enabled

All of the above settings should ensure robust password security.

Recommendation for Contractors

RC30 It is recommended contractors ensure that passwords for user accounts are only known to the owner of that account so that the integrity of the accounts is not compromised.

Recommendation for Contractors

RC31 It is recommended contractors consider implementing network security controls in parallel with the requirements of their information security policy so that access to information is on a "need-to-have/need-to-know" basis. This will provide assurance that access to data, which may be of a personal nature, is only available to those who actually require it.

Recommendation for Contractors

RC32 It is recommend smaller contractors undertake appropriate testing of their network perimeter, at least annually, to gain assurance that it is secure from external attack. This could potentially be conducted under the existing service contracts with external providers.

The cost of performing these tests will vary depending on the complexity of an organisation's network infrastructure. For example, an organisation with a single site and single external connection to the internet would expect to pay upwards of £3,000 whereas a large, multi-site organisation with numerous points of connection to the internet would expect costs to start at £15,000.

Recommendations for Scottish Government

4.3 Listed below are all of the recommendations that apply to the Scottish Government.

Security Policy

Recommendation for Scottish Government

SG1 It would be impractical to stipulate that all smaller contractors should be required to develop their own bespoke information security policy. It is, therefore, recommended that the Government consider updating their contracts to require that all contractors agree to abide by the Scottish Government's information security policies.

SG2 It may also be useful for the Government to make information security compliance part of the assessment criteria of research specifications. This would detail key information security assurance requirements and how each contractor complies with those requirements.

Security Organisation

Recommendation for Scottish Government

SG3 It is recommended consideration be given to drafting a template third party agreement which details the minimum standards the Scottish Government expects contractors to apply when engaging third parties to conduct any aspect of social research work. Consideration should be given to incorporating a requirement within research specifications that sub-contractors formally state their compliance with Section 11 of the Scottish Government's terms and conditions.

Risk Assessment and Asset Management

Recommendation for Scottish Government

SG4 It is recommended that the Scottish Government include within their terms and conditions of contract that there is appropriate encryption of all personal data transmitted by email or other storage media.

Recommendation for Scottish Government

SG5 It is recommended that the Scottish Government mandate that research contractors must use encrypted USB devices when conducting social research work.

Recommendation for Scottish Government

SG6 It is recommended the Scottish Government mandate that contractors must be able to demonstrate that they are using controlled and encrypted USB memory sticks whilst undertaking any social research work. Alternatively, as an interim solution, the Scottish Government should obtain a formal undertaking that USB memory sticks will not be used for Scottish Government social research projects.

Incident Reporting

Recommendation for Scottish Government

SG7 It is recommended, potentially as part of the assessment criteria, that the Scottish Government require contractors to confirm that they will comply with the standards and guidance issued by the Information Commissioner for the management and reporting of data security breaches.

SG8 It is recommended the Scottish Government amend their terms and conditions of contract to require that they must be notified immediately by contractors of any data security incidents relating to social research projects.

Compliance with Security Requirements

Recommendation for Scottish Government

SG9 It is recommended the Scottish Government mandate that all laptops and all other storage media used for the purposes of their social research projects have whole disk encryption. Contractors should be required to formally confirm their compliance with this requirement, potentially within the assessment criteria suggested above.

SG10 It is recommended the Scottish Government make reference to the NHS Scotland Mobile Data Protection Standard as a means of providing guidance to contractors on solutions that could be deployed. The standard can be found at:

http://www.ehealth.scot.nhs.uk/wp-content/documents/mobile-data-protection-standard-pdf3.pdf

Recommendation for Scottish Government

SG11 It is recommended that when awarding contracts for conducting social research projects, the Scottish Government:

- More explicitly define the time period they wish to retain sample data for. This will provide clarity over data retention periods and ensure that all parties are aware of their responsibilities for complying with the Data Protection Act.
- Request contractors to declare that they have deleted all personal data in accordance with contracted requirements.
- Make it a formal requirement for contractors to state their policy on retention and destruction and that this forms part of the assessment criteria of research specifications.

Network and Data Management

Recommendation for Scottish Government

SG12 It is recommended that the Scottish Government consider including the password setting identified above as the minimum standards to be applied by contractors. This could be specified as a requirement of the information security assessment criteria.

5 ANNEX 1

5.1 Detailed below are examples of mechanisms that can be used by contractors to gain assurance that their staff have received, read and understood their information security policy.

Policy compliance software

5.2 This allows organisations to use a software tool to present the policy to staff to read as part of the network login process. The user will then be asked several questions based on the policy they have just read. The user must then achieve a minimum competency score (typically no less than 80%). Only once the competency level has been achieved can the user gain access to the network.

5.3 This has the benefit of promoting the policy whilst providing the organisation with assurance that their staff have read the policy and understood how its requirements are to be applied in day to day working practices. The benefit of these systems is that the organisation can readily demonstrate that all users have received, read and understood the policy. A further benefit of these systems is that they can be used for all corporate policies.

Certificate-based Computer Based Training.

5.4 This actual training mechanism is similar to that used within policy compliance software tools. At the end of the training, ideally conducted during an induction process, the user will be presented with a series of multiple choice questions. The organisation will again define the minimum competency level to be achieved. Once the competency level has been achieved, the user will be prompted to print a certificate showing that they have achieved competency. This should then be passed to a named individual within the organisation who has responsibility for ensuring that all staff complete the test and submit their certificates. From an administrative perspective, this mechanism is more difficult to control.

Paper-based sign-off

5.5 A more basic level of gaining assurance is through having employees sign forms which formally state that they have received a copy of the policy, read it and understood it. This is probably the least effective mechanism as the organisation does not have any formal means of confirming that staff have read the policy and understood its requirements.

6 ANNEX 2

6.1 Detailed below are several options for contractors to consider for improvement of controls for the secure transmission of data.

6.2 An initial step should be the inclusion of the importance of secure data transmission in the formal awareness training and education of staff. This training should seek to raise awareness of the risks associated with failing to secure personal data transmitted via email. To highlight the importance of this, contractors should consider linking the failure to comply with these requirements to their disciplinary code.

6.3 It is essential that staff have clear guidance to allow them to apply the correct security measures to data to which is to be transmitted. To assist staff in making this decision, contractors should produce a decision tree/flowchart which, through a series of questions/challenges defines the most appropriate tool to be used, if necessary, and security (encryption) level to be applied. This could be paper or intranet based.

6.4 Contractors could also give consideration to revision of their business processes relating to transmission of data containing personal information. One option is to require that approval for transmission of personal information must be obtained from a local data protection lead/coordinator prior to it being issued outwith the organisation. The approval could be in the form of an email to the sender or through the local data protection lead/coordinator actually sending the email.

6.5 The final step should be the application of the appropriate security measure, such as data encryption, before the data is transmitted.

ISSN 0950 2254
ISBN 978 0 7559 7463 4
(Web only publication)

www.scotland.gov.uk/socialresearch

RR Donnelley B59917 3/09

GSR
GOVERNMENT SOCIAL RESEARCH
Social Science in Government

ISBN 978-0-7559-7463-4
9 780755 974634