Infrastructure and Projects Authority

Project Assurance Reviews

Data and Information Security – Guide for Review Teams

V1.0

[July 2016]

Reporting to HM Treasury and Cabinet Office

[back of cover – for printed publications, leave this page blank]

This information is also available on the IPA website:
https://www.gov.uk/government/organisations/infrastructure-and-projects-authority

Contents

1. How to use this guide

This guide is intended for Review Team Leaders and Members who will be conducting an assurance review. This document is not a substitute for departmental data and information security policies but should be used as a tool to ensure that reviewers align with the Government's data and information security policies. If you require guidance on programme/project Information Risk Management (IRM) or the Privacy Impact Assessments (PIA), which are mandatory for all new projects that involve the use, disclosure or sharing of personal data, links to the appropriate websites have been provided at the end of this document.

2. Data and Information Awareness

In order to conduct an assurance review, review teams are provided with programme/project documentation which will have the appropriate security markings identified by the programme/project team. At the assessment and planning meetings, the programme/project should be asked to identify any current information and data security practices and agree the detailed practical arrangements for exchange, storage and disposal of programme/project documentation giving regard to the following guidance:

1. **Know what you have** - information is a significant business asset for Government and is key to the delivery of business. All reviewers should understand the application of the Government Security Classification System (see Annex A). This includes awareness of how the data or information in your care should be accessed, stored, posted, emailed and disposed of.

2. **Look after information** - all reviewers have an individual responsibility to ensure that all appropriately marked, sensitive or critical business information provided to them, whether on paper or in electronic form is secure at all times.

3. **Commercial and personal information** – programmes/projects may hold sensitive commercial or personal information. Should reviewers receive any documentation that is commercially sensitive or holds personal information, they are responsible for ensuring that the data or information is secured.

4. **Laptops** – The following advice and guidance is provided for the use of all laptops:

- take care of laptops when in transit - don't leave them unattended;
- avoid drawing unnecessary attention to portable IT equipment especially if travelling or passing through public areas;
- be particularly alert when leaving laptops to go through x-ray machines at airports, etc.;
- never leave any assets or material unattended in a public place;
- lock laptops in the car boot rather than inside whilst on the road but be aware of potential thieves observing you placing a laptop in the boot;
- laptops must not be left in your vehicle overnight;
- store any access key devices away from the laptop and make sure that there is no indication of their purpose; and

- take care of the information when you are travelling e.g. use a privacy screen filter - remember fellow travellers can look over your shoulder if you are working on information private to the programme/project.

5. Transmission of Materials and Data – restrictions for the transmission of data may apply (see Annex A). Reviewers should consider transmission methods at the planning meeting and use alternative options if appropriate (e.g. onsite reading days, hard copy transfer of documents or encryption or documents with password protection).

6. Disposing of Data and Information – as a reviewer, you are responsible for ensuring that all data and information (electronic, hard copy - including notes) that has been provided to you, or generated by you, for the review is disposed of securely or returned to the programme/project team for disposal at the end of the review. Any reviewer that is discovered to be holding any data or information after the review is completed (including the Final Review Report) may have their assurance reviewer accreditation revoked.

3. Procedures for handling a loss of data or information from your care

If you are conducting an assurance review and have become aware that data or information in your care is missing, the following steps must be taken:

- you should identify the last time the information was seen and take appropriate actions to try to recover it (e.g. contacting the lost and found services at the appropriate train station, train services, nearest police station, etc.);
- you must contact the SRO and programme/project team to inform them of the incident and any actions you have taken to try and recover the data and information. The programme/project team may request that further actions be conducted, if deemed appropriate; and
- the Review Team Leader (RTL) who is leading the review should be informed of the incident. The RTL will be responsible for ensuring that the appropriate assurance representative within the Department (i.e. the Departmental Assurance Co-ordinator) is informed of the incident, as well as the appropriate assurance Hub (i.e. IPA, MoD, Devolved Administrations, Local Government).

4. Further information

- Information Commissioner's Office – Privacy Impact Assessments (PIA): https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

- Information on programme/project Information Risk Management: https://www.gov.uk/government/collections/risk-management-guidance

Annex A – Protective markings and document security

Classification Marking	OFFICIAL		SECRET	TOP SECRET
Classification Caveat		SENSITIVE		
What security clearance level is required to access information?	BPSS (Baseline Personal Security Standard).	BPSS. NB: BPSS clearance allows for occasional, limited access to SECRET assets.	SC (Security Check). NB: SC clearance allows for occasional supervised access to TOP SECRET assets.	DV (Developed Vetting).
What material does the classification include?	• Routine correspondence. • Basic/routine personal information. • Routine departmental management information. • Policy advice. • Minutes of meetings.	• Detailed personnel records. • Contractual information considered commercially confidential by the provider. • Policy development/advice to Ministers. • Information about defence or security which could damage capabilities or effectiveness	• Sensitive counter-espionage and counter terrorism related activities. • Joint Intelligence Committee assessments, intelligence summaries. • National Security Policy.	• Highly sensitive intelligence material. • Joint Intelligence Committee assessments.
Can I email it?	Yes, can normally be emailed to non-GSI addresses without further encryption.	Yes, but ensure encryption is used if sending to non-GSI addresses (i.e. beyond .x.gsi, .police.pnn, .nhs or	Only via appropriately accredited secure systems to known recipients. If in	Only via appropriately accredited secure systems to known recipients. If in

	Be aware of sending large amounts of material which may, when aggregated, require encryption.	the Criminal Justice Secure Mail (CJSM) system). When sending on secure networks, best practice is to use password protection of files.	any doubt, ask the review SRO.	any doubt, ask the review SRO.
Can I fax it?	Yes, but make sure the recipient is expecting your fax and check their fax number.	Yes, but make sure the recipient is expecting your fax and check their fax number.	Only via appropriate secure equipment.	Only via appropriate secure equipment.
Can I post it?	Yes, via 1st or 2nd class post. NB: Items posted to Northern Ireland should not have any markings which designate that they come from a government department.	Yes, doubled enveloped via Royal Mail Special Delivery, obtaining a signature upon delivery.	Only via appropriate departmental distribution service.	Only via appropriate departmental distribution service.
Can I take papers out of the office or work on them at home if they cannot be worked on remotely?	This is to be avoided if possible, consider other alternatives. If you take such material out of the office it must be carried in a container (ideally a lockable one) which does not allow anyone to see the material.	This is to be avoided if possible, but if necessary, you must have the prior agreement of your line manager (or the SRO in the context of reviews). If you take such material out of the office it must be carried in a container (ideally a lockable one)	This is to be avoided, but is possible in rare and exceptional circumstances where no other option exists. You must obtain the prior agreement of your Head of Management Unit.	This is to be avoided, but is possible in rare and exceptional circumstances where no other option exists. You must have the prior agreement of your Head of Management Unit and Departmental Security Officer and a risk assessment must also be undertaken beforehand.

		which does not allow anyone to see the material.		
How do I store it?	On official premises, lock OFFICIAL assets (including papers and equipment) away when not in use. At home, lock OFFICIAL assets away when not in use.	Lock OFFICIAL assets away when not in use. At home, follow departmental guidelines established when agreement to remove the papers from the office was given.	Locked in an approved container (e.g. Mersey cabinet) on official premises.	Locked in an approved container (e.g. Mersey cabinet) on official premises.
How do I dispose of it?	Return documents to the office for disposal in accordance with departmental guidelines.	Return documents to the office for disposal in accordance with departmental guidelines.	Return documents to the office for disposal in accordance with departmental guidelines	Return documents to the office for disposal in accordance with departmental guidelines.

The information provided above should be seen as a guide only. Arrangements for data and information security for the review must be agreed with the programme/project team at the assessment and planning meetings. The storage, disposal and transmission of information, including that classified as Secret and Top Secret should be discussed and agreed with the programme/project team at the assessment and planning meetings. Where deemed appropriate by the programme/project team and in consultation with the review team, the review team may be required to have an internal reading day within the programme/project office before the review is conducted.