FACT SHEET 9
SECURITY REQUIREMENTS

Security Requirements

The Licensee must comply at all times with the following security requirements in relation to the Datasets with a classification of unclassified – (DLM) for General Release and unclassified – (official use only) for Unconfidentialised datasets:

> Only allow the Unit Record Data from the Datasets to be viewed by Authorised Users. Store all complete or partial dataset/s, in accordance with the baseline security controls detailed within the Australian Government Protective Security Policy Framework (PSPF) and the Australian Government Information Security Manual (ISM) applicable to Australian government information which requires some level of protection. As amended from time to time.
>
> Further information relating to the Protective Security Policy Framework and the Information Security Manual can be found on the following websites:
>
> - Protective Security Policy Framework: http://www.protectivesecurity.gov.au
> - Information Security Manual: http://www.asd.gov.au/infosec/ism/

The Protective Security Policy Framework and Information Security Manual maybe updated from time to time. The Licensee must regularly check for updates to these documents and comply with the provisions set out in the latest version.

Minimum Security Standards

1. The following ISM standards are the minimum requirements for users of the Department of Social Services (DSS) longitudinal Datasets these include but are not limited to:

   a. Agencies must register all ICT equipment and media with a unique identifier in an appropriate register
   (**control 0336** of ISM (control last updated Sep 2011))

   b. To destroy media, agencies must either:
   - Break up the media
   - Heat the media until it has either burnt to ash or melted
   - Degauss the media

   (**control 0364** and see 0366 of ISM (control last updated Nov 2010))

   c. Agencies using passphrases as the sole method of authenticating a user must implement a passphrase policy enforcing either:
   - a minimum length of 13 alphabetic characters with no complexity requirement; or
   - a minimum length of 10 characters, consisting of at least three of the following character sets:
     - lowercase alphabetic characters (a–z)
     - uppercase alphabetic characters (A–Z)
     - numeric characters (0–9)
     - special characters.

   (**control 0421** of ISM (control last updated Feb 2014))

d. During operational and non-operational hours, ICT equipment and media needs to be stored in accordance with the *Australian Government Physical Security Management Protocol*.

The physical security requirements of the Australian Government Physical Security Management Protocol can be achieved by:

- ensuring ICT equipment and media always resides in an appropriate security zone
- storing ICT equipment and media during non-operational hours in an appropriate security container or room
- using ICT equipment with a removable hard drive which is stored during non-operational hours in an appropriate security container or room as well as sanitising the ICT equipment's Random Access Memory (RAM)
- using ICT equipment without a hard drive as well as sanitising the ICT equipment's RAM
- using an encryption product to reduce the physical storage requirements of the hard drive in ICT equipment to an unclassified level as well as sanitising the ICT equipment's RAM

Agencies must ensure that ICT equipment and media with sensitive or classified information is secured in accordance with the requirements for storing sensitive or classified information in the *Australian Government Physical Security Management Protocol.*

(**control 0161** of ISM (control last updated Sep 2011))

FAQ

1. The ISM p.4 states under "Authority to approve non-compliance" that only certain authorities have the ability to approve non-compliance. When the ISM refers to Agency Head (AH) is that the head of an organisation or the head of DSS? When the ISM refers to the Accreditation Authority (AA) is that the applicable person within the organisation or the DSS Accreditation Authority?

   As the ISM is the standard which governs the security of Government ICT systems, the Agency Head (AH) and Accreditation Authority (AA) is referring to the DSS AH and AA. The ISM is written specific to Government Agencies.

2. Are all of the controls listed in the PSPF and ISM applicable to an organisation? Which controls are applicable and must be implemented?

   Refer to the ISM System Control Checklist matrix that reflects the relationship between the security classification of data (in this instance 'UNCLASSIFIED' or 'GOVERNMENT') and the system controls from the ISM. It lists each control in the order it is found in the layout of the ISM. The spread sheet lists:
   - The section of the ISM from which the control comes e.g. 'Evaluating and treating information security risks'
   - The control number e.g. '1203'
   - Whether compliance with the control is mandatory or recommended e.g. 'MUST'
   - If the control is relevant to the particular security classification of the data e.g. 'GOVERNMENT' (shown as G in the spread sheet). I have hidden the other columns. GOVERNMENT classification pertains to systems containing UNCLASSIFIED but sensitive information not intended for public release. This is the only one we are concerned with for this data.

   The matrix needs to be read against the ISM, by using the corresponding control code in the spread sheet to find and read about the control in the ISM.

   Controls with a 'must' or 'must not' compliance requirement

   Controls with a 'must' or 'must not' compliance requirement are mandatory.

   Controls with a 'should' or 'should not' compliance requirement

   Controls with a 'should' or 'should not' compliance requirement are recommended. However, valid reasons should exist to vary from the controls.

   In the spread sheet, **where the 'G' column reads 'No',** the corresponding security control can be disregarded, as the control is not relevant to data classified as GOVERNMENT.

   You may wish to add in another column to record how the control is being met e.g. for the 'Evaluating and treating information security risks' controls, a number could be achieved through a Risk Evaluation Plan.

3. If a control is applicable, does this mean that the control must be implemented for the entire organisation or just to the part of the organisation (i.e. division) that is

dealing with DSS's information? For example, control 0380 (p.142 of the ISM), would it apply to all organisation computers or to only the computers used to store, transmit and process DSS's information?

The answer to this depends on the design of the organisations network. If the servers/machines that are storing, processing or transmitting DSS's data are not segmented from the rest of the network, then it is likely that the relevant controls from the ISM would apply to the whole of the network. If the organisation is able to outline in more detail how the network is arranged with respect to the handling of this data, a more informed answer can be provided.

4. Is it possible to limit the scope of the controls through, for example, segmenting the network that is being used to store, transmit or process DSSDSS's information? If so, how can this be achieved?

   DSS's Cyber Security section is able to provide some limited advice to assist with network segmentation if need be. Advice can be provided concerning some best practice. Limited guidance on Network Security and other relevant sections of the ISM, with respect to their network, can also be provided. An initial understanding of the organisations network design will inform this.

   Forward queries in the first instance to: longitudinalsurveys@dss.gov.au