Department of Culture and the Arts
Government of Western Australia

State Records Office of Western Australia

SRO Guideline

SANITIZING DIGITAL MEDIA AND DEVICES

An Information Management Guideline for State Organizations

State Records Office of WA
Perth: Western Australia

July 2011

TABLE OF CONTENTS

PURPOSE

The purpose of this Guideline is to assist State organizations in ensuring that data stored on digital media and devices has been sanitized ready for disposal upon decommissioning. This Guideline should be read in conjunction with State Records Commission Standard 8: *Digital Recordkeeping*.

This Guideline supersedes *SRO Guideline: Sanitizing of Hard Discs and Magnetic Media* (2008).

BACKGROUND

State organizations regularly replace or dispose of computing equipment containing media for storage, as well as self contained storage media.

Computing equipment may include laptops, servers, desktop computers, faxes, scanners, printers, photocopiers and multi-function devices.

Self contained storage media may include magnetic based (such as floppy discs or magnetic tape); optical media (such as CD's and DVD's); flash media including USB flash drives and memory cards (eg: in cameras or mobile phones) and mobile phones and PDA devices.

Before these items are disposed of, the storage media should be sanitized to ensure that sensitive information stored on them cannot be retrieved or reconstructed. The technique for treating these media may vary according to a risk assessment of the data contained on them. The nature of some of these media means that the only reliable method of sanitizing is to physically destroy the media.

SCOPE

This guideline applies to all State organizations and is intended to be of use to both Records Management and Information Technology professionals.

LEGAL DESTRUCTION

Under the *State Records Act 2000*, a State organization's records, regardless of format, are to be retained and disposed of in accordance with an approved disposal authority. The State Records Commission is the authorizing body for disposal authorities.

Prior to decommissioning systems, State organizations should refer to State Records Commission Standard 8 (Digital Recordkeeping) and their approved Retention and Disposal Schedule. It is the responsibility of the principal officer of a State organization to ensure that data stored on digital media and devices is only destroyed in accordance with disposal authorities approved by the

State Records Commission and not inadvertently destroyed or exposed when media or systems are decommissioned without data being migrated.

The destruction of government information should be done completely and in conjunction with a risk assessment of the data.

RISK MANAGEMENT

Before embarking on the disposal of data storage media, State organizations must undertake a risk analysis of the data contained on these systems to determine the sensitivity of the content and the most appropriate method of sanitization. Western Australia does not have a formal data classification system so agencies will need to assess the sensitivity of data.

As part of their risk management, State organizations should periodically sample the media they are sanitizing to ensure that their process for sanitization is functioning correctly.

OUTSOURCING

State organizations choosing to use CUA 47110 to outsource the disposal of equipment that has a data storage media component should ensure that the company performing the disposal work is performing media sanitization in accordance with this guideline. Organizations should also assess as part of the risk management process whether it is appropriate to outsource the sanitization of media to a third party or to perform this function internally before sending equipment to a third party for disposal. For equipment containing information that is highly sensitive, sanitization should be performed by the State organization prior to outsourcing the disposal of the equipment.

HARD DISCS AND MAGNETIC MEDIA

Reformatting magnetic media does not ensure that the data once stored on it cannot be recovered at a later time.

Discs or backup tapes from servers may contain highly sensitive information and in these cases should be sanitized using the physical destruction method.

Discs from printers, faxes, scanners, photocopiers or multi-function devices may contain highly sensitive information which has been digitally copied or digitized and stored on the devices' hard drive, and in many cases it will be difficult to determine what remains stored on these discs. These machines should therefore be sanitized using the physical destruction method.

- Use **Physical Destruction** for data deemed to be highly sensitive.
- Use **Degaussing** for data deemed to be moderately sensitive.
- Use **Overwriting** for data deemed to be non-sensitive.

OPTICAL MEDIA

As optical media is not magnetic, it cannot be sanitized by degaussing. Many types of optical media are "write once" media (eg: CD-R, DVD-R) and are not able to be overwritten. The only way to ensure the sanitization of optical media is to physically destroy the item.

- Use **Physical Destruction** or Incineration for data deemed to be highly sensitive.
- Use **Abrasion** for data deemed to be moderately sensitive or non-sensitive.

FLASH MEDIA AND SOLID STATE DRIVES

Reformatting flash media does not ensure that the data once stored on it cannot be recovered at a later time.

Memory cards in mobile phones may contain highly sensitive information and in these cases should be sanitized using the physical destruction method.

- Use **Physical Destruction** for data deemed to be highly sensitive.

- Use **Overwriting** for data deemed to be moderately sensitive or non-sensitive.

MOBILE PHONES AND PDA DEVICES

Manually deleting data from a mobile phone or PDA device does not ensure that the data once stored on it cannot be recovered at a later time. A mobile phone may contain highly sensitive information that has arrived via email. The only method which can give surety of the sanitization of these devices is the physical destruction of the device.

Where possible, it may be more prudent to store any data for the mobile phone or PDA device on an internal flash media storage device, and sanitize that item upon decommissioning or disposal. See also – Flash Media.

- Use **Physical Destruction** for data deemed to be highly sensitive.
- Use **Deletion** for data deemed to be moderately sensitive or non-sensitive.

HYBRID DRIVES

Hybrid drives are a combination of standard magnetic media and flash media drive. The components of these drives should be treated in the ways outlined above for magnetic media and flash media.

METHODS OF DESTRUCTION

There are several methods to provide greater certainty that data cleansed from digital media and devices cannot be reconstructed. These methods differ in the manner of application and the level of assurance that data cannot be reconstructed or retrieved. The method chosen will be determined by the risk analysis, conducted prior to disposal, and the level of sensitivity of the content of the stored data.

Media should be sanitized according to the degree of sensitivity of the **most** sensitive information it contains.

1. Physical Destruction

Where data is determined to be **highly sensitive**, the Physical destruction method is recommended.

Where it is difficult to determine whether or not data may be highly sensitive, the Physical destruction method is recommended.

Recommended methods of physical destruction of media include:

1. Shredding or otherwise breaking the media into small pieces; or
2. Application of corrosive agents to the media; or
3. Melting of media in a furnace.

When using a method of physical destruction of media, it is essential that any relevant Occupational Health and Safety measures are followed.

NB: These methods of data destruction will render the media unusable after the operation is performed.

2. Incineration

Where data is determined to be **highly sensitive**, the incineration method may be considered appropriate.

Incineration of media must reduce the media to a fine particulate or ash.

When incinerating media, it is essential that any relevant Occupational Health and Safety measures are followed.

NB: This method of data destruction will render the media unusable after the operation is performed.

3. Degaussing

Where data is determined to be **moderately sensitive**, the Degaussing method may be considered appropriate.

Degaussing is the application of a strong magnetic field to magnetic media to randomize the patterns of data on the media. Commercial degaussing units can be purchased to perform this function.

NB: Whilst there is the possibility of rendering the media unusable after this operation is performed, this method is not a means of destruction and data may be retrievable.

4. Overwriting

Where data is determined to be non-sensitive, the Overwriting method may be used.

This method involves a process of overwriting patterns of data across the entire media to ensure that data stored on it has been replaced with new, meaningless data. To ensure that there are no remaining patterns of data on the media it is recommended that the following steps are taken:

1. Write a series of zeros or ones to the entirety of the media; then
2. Write a series of ones or zeros (whichever not used in the step above) to the entirety of the media; then
3. Write a series of random data to the entirety of the media.

NB: This method is not a means of destruction and data may be retrievable.

5. Deletion

Where data is determined to be **moderately sensitive or non-sensitive**, the Deletion method may be used.

This method involves manually deleting all data on the device and performing a full or “cold” manufacturer’s reset to put the device back to default settings.

NB: This method is not a means of destruction and data may be retrievable.

6. Abrasion

Where data is determined to be **non-sensitive**, the abrasion method may be considered appropriate.

Abrasion is the removal of the information bearing layers of a piece of optical media using a commercial optical disc grinding device.

NB: Whilst there is the possibility of rendering the media unusable after this operation is performed, this method is not a means of destruction and data may be retrievable.

APPENDIX A – Table of Media and Sanitization Methods

	Highly Sensitive	Moderately Sensitive	Non-sensitive
Hard drives	Physical destruction	Degaussing	Overwriting
Tapes	Physical destruction	Degaussing	Overwriting
CDs and DVDs	Physical destruction	Abrasion	Abrasion
Memory cards (eg: SD cards, MMC cards, Mini SD cards, CF cards)	Physical destruction	Overwriting	Overwriting
USB drives	Physical destruction	Overwriting	Overwriting
Mobile phone* (including smartphones)	Physical destruction	Deletion	Deletion
PDA* (eg: Palm Pilot)	Physical destruction	Deletion	Deletion
Hybrid drives	Each component as per its type listed above (eg: magnetic drive and flash media drive)	Each component as per its type listed above (eg: magnetic drive and flash media drive)	Each component as per its type listed above (eg: magnetic drive and flash media drive)

* Note that these devices may contain a memory card which can be sanitized according to the directions for Flash Media.