



Department of Culture and the Arts
Government of Western Australia

State Records Office of Western Australia

SRO Guideline

SANITIZING OF HARD DISCS AND MAGNETIC MEDIA

**A Recordkeeping Guideline for
State Organizations**

**State Records Office of WA
Perth: Western Australia**

February 2008

TABLE OF CONTENTS

PURPOSE	3
BACKGROUND	3
SCOPE	3
LEGAL DESTRUCTION	3
RISK MANAGEMENT	3
OUTSOURCING	4
SANITIZING OF HARD DISCS AND MAGNETIC MEDIA	5

PURPOSE

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

BACKGROUND

State organizations regularly replace computing equipment, including laptops, servers and desktop systems, as well as other magnetic media (such as magnetic tape) used to store electronic data.

Before these items are disposed of, their 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.

SCOPE

This guideline applies to all State organizations and is intended to be of use to 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 magnetic media 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 hard discs or other magnetic 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.

State Records Guideline – Sanitizing of Hard Discs and Magnetic Media

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 outsource the disposal of equipment under CUA 5105 that has a hard disk or magnetic 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 information that is highly sensitive, sanitization should be performed by the State organization prior to outsourcing the disposal of the equipment.

SANITIZING OF 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.

There are several methods to provide greater certainty that data cleansed from magnetic media 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. For example, discs or backup tapes from servers may contain highly sensitive information and in these cases should be sanitized using the physical destruction method.

Physical destruction

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

Recommended methods of physical destruction of magnetic media include:

1. Shredding or otherwise breaking the media into small pieces; or
2. Application of corrosive agents to the media;
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: This method of data destruction will render the media unusable after the operation is performed.

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.

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.