Australian Communications-Electronic Security Instruction 33 (ACSI 33)

Point of Contact: Customer Services Team

Phone: 02 6265 0197 Email: assist@dsd.gov.au

HANDBOOK 6

MEDIA SECURITY

Version 1.0

Objectives

601. This handbook deals with the issues of security of media as used in Government IT systems. Specifically, it discusses:

a. The risk of National Security or Non-National Security information being disclosed to unauthorised persons through the disposal of failed or obsolete equipment or media, and the countermeasures available to minimise this risk.

b. References to the physical security protection of storage media, as used in operational systems.

Terminology

602. Considerable information may still be obtained from computing equipment and media, which have either failed or outlived the purpose for which they were acquired. In general there is no known method short of total destruction which will **completely** remove all traces of the information borne by memory devices (including volatile storage such as Random Access Memory (RAM)) or magnetic media. However, some sanitisation measures can significantly reduce the risk of information being recovered from used media. When considering the disposal of media and equipment it is important to recognise the difference between "sanitisation" and "declassification".

a. **Sanitisation** is the process of erasing as far as is possible the information from the media or equipment. The process of sanitisation does not automatically change the classification of the media or equipment.

Note that sanitisation does not involve destroying the media or equipment.

b. **Declassification** is the removal or reduction in the classification of the media or equipment. The decision to declassify should be preceded by an assessment of the risk of improper disclosure of any information remaining on the media or equipment, should the declassification take place. In considering risk associated with declassification, it is important to take into account the resale value of the asset(s), the destination of any released media (and therefore the likelihood of compromise), the serviceability of the media which may directly relate to the resale value, and any contractual obligations.

603. Media or equipment that has carried classified information must always be afforded the classification level of the most highly classified information that it has ever processed or stored, until appropriate sanitisation and declassification take place. The remainder of this handbook discusses, in part, sanitisation requirements for specific types of equipment and media. Users of this handbook should note that DSD can advise on equipment and media not covered in the remainder of this handbook.

Degaussing

604. Degaussing, also referred to as demagnetising, is a procedure that reduces the magnetic flux density to zero by applying a reverse magnetising field. Degaussing renders any previously stored data on magnetic media unreadable. Degaussing is the most reliable method of purging magnetic media short of destruction. Equipment suitable for degaussing is listed in the **Evaluated Products List (EPL)**. Although the EPL categorises degaussers into Type I and Type II devices, it is essential that a degausser be chosen based on the target media rather than the "Type" of degausser. Additionally, if an approved degausser is used, it is important to verify that it is configured and working correctly. DSD should be consulted if a degausser is required to sanitise media.

Magnetic Media Overwrite

605. The standard method used to declassify by overwriting is to write over every addressable location with one pattern (usually binary 'ones') and then with the complementary pattern (eg binary 'zeros'). This cycle of overwrites is then repeated a number of times, where the number is based on the requirements for declassification and/or the risk assessment. Note that any binary pattern can be used, as long as the opposite or complementary pattern is written alternately, for the given number of cycles. In order to ensure that the media overwrite procedures are correctly undertaken, the following steps are recommended:

a. Overwrite all the data bit locations with a pattern such as binary zeros, and verify that it has occurred.

b. Overwrite all the data bit locations with binary ones (or the complement of whatever pattern was used in the previous step), and verify that it has occurred. Verification of the overwrite may be accomplished by reading all or a sample of the information (proportion based on a risk

assessment), and ensuring that no other characters can be detected.

c. Repeat the above steps a number of times, based on the requirements for declassification and/or the risk assessment.

606. Failed classified devices cannot be effectively sanitised and declassified by overwriting. It must be assumed that all the data held at the time of failure could be read easily. If a repair cannot be effected in a secure facility, DSD advice must be sought if it is required that the media be disposed of as a declassified item.

Laser Printer and Copier Drums

607. Laser printer drums may be sanitised and declassified to "Unclassified" by printing a quantity of UNCLASSIFIED (eg blank) pages designed to exercise the whole drum after its last use for classified printing.

Volatile Media

608. Memory devices and other volatile storage retain some information even after the power has been lost, although at such a low level that sophisticated methods are needed to recover it. Unless very highly classified, volatile memory may be sanitised sufficiently by the removal of all power (including all battery power), and earthing the device. A decision on whether to release the item to uncleared persons or destroy it must be based on a risk assessment taking into account the quantity and classification of the data the device bears.

Physical Security and Destruction Methods

609. Paper, microfiche, microfilm, CDs and related storage media cannot be sanitised and must be destroyed in an approved disintegrator or by burning/smelting under the control of a suitably cleared person. Destruction of volatile media should be by means of an approved method. Destruction of hard disk and volatile memory should occur by melt, smelt, grind, or smash. Floppy disk media should be destroyed by an approved method. Approved microfiche and film destruction systems are listed in the Security Equipment Catalogue.

610. All media that is used for storage of National Security and Non-National Security classified information, whether fixed or removable, should be accorded the physical protection standards required by the PSM. Guidelines on physical security requirements, whether building, room or perimeter security, are contained in **Handbook 14 - Physical Security** and will not be replicated in this document. To this end, media and equipment should be treated as hard copy media for the purpose of considering physical security storage requirements. Media or equipment that has carried classified information must always be afforded the classification level of the most highly classified information that it has ever processed or stored, until appropriate sanitisation and declassification takes place.

Grades of Sanitisation

611. The following grades of sanitisation have been included to assist in determining the level of effort that should be allocated to such a task. They are not

definitive, and when implementing sanitisation procedures should be used as a guide. There are three categories of media included in the following grades, which are generally the most common. These are "magnetic media", "laser printer/copier drums" and "volatile memory". Volatile memory includes solid state memory that loses data when power is removed (eg RAM), but does not include devices that do not lose data (eg EEPROMs).

a. **Grade 0**

i. Magnetic media not sanitised.

ii. Laser printer/copier drums not sanitised.

iii. Volatile memory devices not sanitised.

b. **Grade 1**

i. Magnetic media sanitised via an EPL approved degausser or single overwrite method.

ii. Laser printer/copier drums not sanitised.

iii. Volatile memory devices not sanitised.

c. **Grade 2**

i. Magnetic media sanitised via an EPL approved degausser configured as per DSD recommendations; or double or triple overwrite method, subject to the outcomes of a risk assessment. The risk assessment should take into account the cost (or resale value) of the media, the amount of classified information stored on the media and the serviceability of the media. A declassification decision following sanitisation should be no more than two levels of classification below the original classification of the media.

ii. Laser printer/copier drums sanitised via approved method.

iii. Volatile memory devices sanitised via approved method.

d. **Grade 3**

i. All magnetic media destroyed

ii. Laser printer/copier drums sanitised via approved method.

iii. Volatile memory devices sanitised via approved method, subject to the outcomes of a risk assessment. The risk assessment should take into account the cost (or resale value) of the media, the amount of classified information stored on the media and the serviceability of the media.

e. **Grade 4**

i. All magnetic media destroyed.

ii. All laser printer/copier drums destroyed.

iii. All volatile memory devices destroyed.