New Zealand Security of Information Technology Publication 207

DECLASSIFICATION OF STORAGE MEDIA

CHAPTER 1

MAGNETIC STORAGE MEDIA

Introduction

101. Systems which process classified or sensitive information generally use magnetic storage media for temporary and permanent storage. Once the information on the storage media is no longer required the media must be declassified prior to disposal or reuse to protect against recovery of previously stored material. The correct application of the procedures described in this publication for declassification and destruction will, to an acceptable level of assurance, provide protection against electronic scavenging of discarded information.

102. Destruction rather than declassification should be carried out where:

a. the cost of the storage media is low;
b. the media has at some stage stored information classified TOP SECRET; or
c. the media has at some stage stored information classified SECRET and, subsequent to declassification, is to be disposed of outside New Zealand.

103. The information provided in this chapter applies to all types of magnetic tape, fixed and removable hard disks, and floppy diskettes.

Reusing Media

104. New or properly declassified media may be used without restriction. Once used, however, media are to be classified at the highest level of information stored and are to be protected accordingly. Users must be cleared for access to all material which has been previously stored on the media.

Methods of Declassification

105. A storage medium is a document classified to the highest level of information ever stored. Depending on the media and the classification of information stored, either degaussing or overwriting procedures can be used to declassify the media. Similar considerations apply to the storage of sensitive information.

106. Any special procedures defined for declassification of specific types of information will take precedence over the general procedures stated below.

Assurance

107. Declassification can be carried out either to clear or to purge storage media. Clearing provides assurance that under normal operating conditions, even with the use of sophisticated software, it is not possible to recover the cleared data; however, some data may still be recoverable through analysis of the storage media using special laboratory equipment. Purging provides assurance that data cannot be recovered from the storage media even with the use of special laboratory equipment.

Declassification of Media By Degaussing

108. Degaussing, or demagnetising as it is sometimes known, is the best method of purging magnetic storage media. Degaussing is approved for declassification of all forms of magnetic media which have held classified or sensitive information.

109. While older types of magnetic disk contained physical timing marks, modern sealed magnetic disks contain electronic timing track information which will be removed when the disk is degaussed. Because such information can be restored only at the manufacturers facilities the alternatives of overwriting or destruction may be more appropriate. Most floppy diskettes can be degaussed as they use a physical timing mark (a hole in the diskette).

110. Degaussing equipment is available for magnetic tape, hard disks, and floppy disks. In all cases care should be taken to ensure that the equipment used is appropriate for the type of magnetic material. The manufacturer's procedures for use of the equipment should be strictly adhered to and the equipment should be regularly calibrated.

Declassification of Media by Overwriting

111. An alternative method of clearing magnetic media is to overwrite every data location including, where relevant, boot record and file table space, followed by reformatting. This procedure does not provide as high a level of confidence as degaussing but is approved where degaussing is not possible. Overwriting is not adequate for purging magnetic tape or floppy disks but is acceptable for purging hard disks. The overwriting software should be protected to the same level as the media being declassified in order to provide adequate assurance of software integrity.

112. Departments may write special software to overwrite media, but the software should operate at least as stringently as the routine described by the following pseudocode:

- Repeat 3 times
- Write 00H in every addressable location
- Write FFH in every addressable location
- Write random values in every addressable location

113. It should be noted that utilities such as XR25 operate by overwriting only those disk clusters not being used by a file. While this feature is necessary in situations where the disk contains files that are to be kept, care should be taken that temporary, swap, and print-spool files also remaining on the disk do not contain copies of the information being sanitised.

114. The effectiveness of the overwrite procedures may be reduced through equipment malfunctions such as read/write head misalignment or head failure. If the overwriting software identifies errors when attempting to overwrite (e.g. bad blocks), or if there is any doubt about the reliability of the overwriting software or hardware, degaussing or destruction procedures should be used.

115. It should be noted that reformatting a hard or floppy diskette does not necessarily overwrite the data on the disk. REFORMATTING IS NOT AN APPROVED MEANS OF DECLASSIFYING MAGNETIC DISKS.

Destroying Media

116. When media has been used for the storage of material classified TOP SECRET, where the media has been used for the storage of information marked SECRET and is to be disposed of outside New Zealand, or when declassification through degaussing or overwriting is not possible, media must retain the highest classification of any information previously recorded. When no longer required the media must be destroyed.

117. Destruction of magnetic material should be undertaken by fire and any residue from burning should be reduced to minute fragments. An alternative to destruction by fire is destruction by acid. Magnetic disks can be immersed in concentrated hydriodic acid (55% - 58% solution) until the magnetic material has been totally dissolved leaving only the aluminium or plastic platter.

118. Shredding is not approved for destruction of floppy diskettes. Not only can shredding of plastic material damage the shredder, but the information density of magnetic media is such that a strip of shredded material could contain significant information.

Repair of Damaged Media

119. Damaged media that have contained classified or sensitive information must be repaired by cleared technicians and throughout repair protection must be provided for the information stored on the media. Faulty storage media that can be repaired only at an uncleared vendor depot must be declassified by degaussing before being sent for repair. Where this is not possible the media must be destroyed rather than repaired.

Recording Declassification and Destruction

120. In all cases where storage media are destroyed or declassified the action should be undertaken by an authorised staff member in the presence of a witness, and a certificate of declassification should be completed and passed to the departmental security authority. This certificate should indicate:

a. a description of the medium (type, manufacturer, model, serial no);
b. the original and final classification, and intended destination of the medium;
c. the reason for declassification;
d. a description of the declassification procedure, detailing as appropriate the degausser used, the identification of overwriting software, or the destruction process; and
e. the names and signatures of the departmental staff carrying out and witnessing the activity.

Further Advice

121. Products approved for degaussing or overwriting magnetic storage media are listed in the publication *NZCSIM 402: Preferred Product List* . NZ Government departments can obtain further advice or assistance on declassification or destruction of magnetic storage media from the GCSB.

CHAPTER 2

OTHER STORAGE MEDIA

Optical Media

201. Neither write-once/read-many (worm) nor rewritable optical disks can be declassified. Once used to store classified or sensitive data they should retain the highest classification of any information previously recorded.

202. When no longer required, optical material that has ever held classified or sensitive information should be destroyed by fire and the destruction recorded as detailed in para 119.

Semiconductor Memory

203. Random access semiconductor memory that has been used for processing information up to SECRET may be declassified by standard overwriting in the same manner as for magnetic disks (see para 112). Ultraviolet programmable read only memory (UVPROM) chips can be cleared or purged adequately using standard overwrite procedures and ultraviolet light.

204. Semiconductor memory that has been used for processing information marked TOP SECRET may be declassified by the following procedure:

a. overwrite the memory using the standard procedure described in para 112;

b. remove all power (including batteries) from the circuit board; then

c. leave the device powered ON in the unclassified state for 72 hours.

205. Faulty semiconductor memory that has ever held information classified SECRET or above should be destroyed by fire and the destruction recorded as detailed in para 119.

Electrostatic Drums

206. Photocopiers and laser printers are examples of equipment that uses electrostatic principles for printing. During the printing process information is stored on an electrostatic drum.

The drum can be declassified by printing six or more blank pages.

Transient Storage

207. Items such as printer ribbons which store classified or sensitive information transiently as part of their operation must be destroyed by fire and the destruction recorded as detailed in para 119.