



Media Clearing and Sanitization

Introduction

Clearing and sanitizing electronic storage media are the processes for rendering the data stored on an electronic data storage device inaccessible and unreadable.



Explanation of Processes

Clearing – Clearing must be adequate to prevent data recovery using tools readily available on the Internet. Simply deleting or erasing the files or formatting a disk does not clear the media, because commands such as undelete or unformat may permit the recovery of the data. The clearing process is not expected to be proof against “hands-on” recovery methods using specialized IT utilities or laboratory techniques. For this reason, cleared media must be retained within security environments appropriate to the level of classification of the cleared data the media once contained, and cannot be considered for declassification.

Sanitization - Sanitizing is the process of erasing or destroying storage media in a manner that precludes any reasonable hope of recovery of the data – i.e., the risk of compromise following sanitization is low or non-existent. In addition to destroying the data, the sanitization process includes the manual removal of external indications that the device once contained sensitive data. Electronic data storage devices that have been sanitized may be declassified and disposed of as unclassified waste or as surplus equipment for sale or recycling.

Clearing and Sanitization Methods

Overwriting – Clearing Method –Triple overwrite (RCMP-recommended method) is a process involving three passes of overwrite software in accordance with RCMP overwrite criteria

Physical Destruction – Sanitization Method - Physical destruction and deformation involve the use of tools such as sledge hammer, nail gun, vice, etc, to cause extreme physical damage to a storage device in order to delay, impede, or discourage an attacker from attempting to recover data from it.

Degaussing – Clearing Method - Degaussing is the application of magnetic force of sufficient power to erase all data on a given magnetic data storage device.

Encryption – Clearing Method - Encrypting all data on the media and destroying all means of decrypting renders the information inaccessible and unreadable. Employees should ensure encryption is according to Government of Canada standards for the level of classification of the information on the media.

Final Recommendations

The appropriate method to clear and/or sanitize storage media should be identified through a comprehensive Threat and Risk Assessment (TRA). Storage media must be treated at the appropriate classification of the data. Storage media can be declassified through effective sanitization methods.

