Validation of data retention in relation to the data retention policy prior to sanitization. It

Media Sanitization Methods

The computing environment is constantly moving forward

McGill Sanitization Requirements

The removal of data remnants is an important issue that shall be taken into consideration when disposing of equipment. In many cases, even when files are deleted or disks formatted, data may still remain. This data may include confidential and/or sensitive documents, saved credentials, product keys, etc. Such data remnants have led to several high profile data loss incidents, thus a proper data cleansing process shall occur to ensure that data does not “escape”, even when disks are not to be reused.

Disposal and transfer of IT Equipment must abide by the guidelines specified in McGill’s IT Asset Management Regulation:
http://www.mcgill.ca/procurement/files/procurement/mcgill_it-asset_reg.pdf
All Electronic data must be sanitized as per the minimum procedure outlined in the table set forth below:

Data Classification Guidelines

Digital Media Types and Data Sanitization Methods

Due to the large breadth of data storage, minimum sanitization methods for McGill data should follow the recommendations in NIST SP 800-88 Rev. 1 Appendix A (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf).

Internal Disk Drives (ATA, SCSI)

While actions such as formatting and deletion appear to remove data from disk, this is not necessarily the case. In fact, for performance reasons many operations only remove the pointer to a file and in fact leave much of the data

Purge: Purging should be performed via the ATA Sanitize command, ATA Secure Erase command or with Instant Secure Erase (if available). Validation of the clearing of data must be performed to ensure proper purging.

Destroy: Destruction/disposal of the media must be performed by a certified disposal company. A certificate of destruction must be provided.

Removable Media

External HDD/SSD

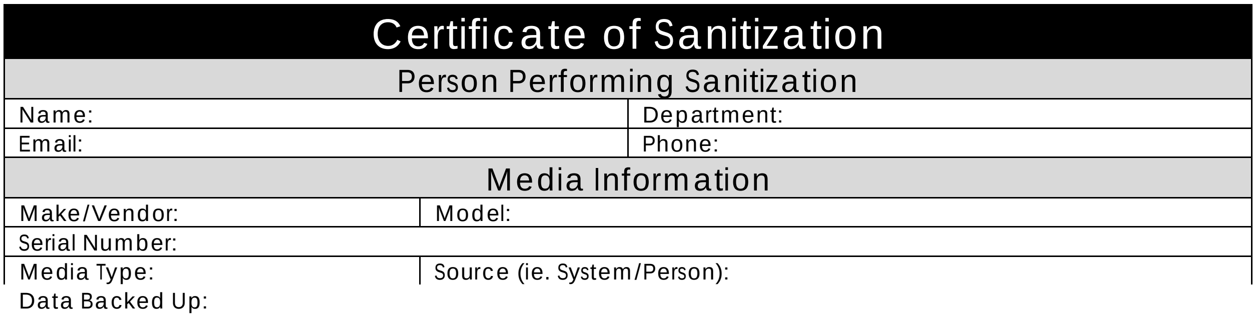
Format: Using the operating system own format functionality to erase all bookkeeping information on the media.

Clear: At minimum, a single pass of a fixed pattern (such as all zeros) should be written to the entire disk and validation of the overwriting must be performed. Multiple passes with more complex values may be used to further ensure proper clearing of the data.

Purge: Purging may not be possible depending on the device. Purging should

Purge:

Example of Sanitization Certificate



Certificate of Sanitization	
Person Performing Sanitization	
Name:	Department:
Email:	Phone:
Media Information	
Make/Vendor:	Model:
Serial Number:	
Media Type:	Source (ie. System/Person):
Data Backed Up:	