# McGill University
# Digital Media Sanitization Guidelines

Document version 1.1

Publication date: 25 April  2016

Last updated: 25 April 2016

# Contents

Objectives ........ 3

Media Sanitization Methods ........ 5

McGill Sanitization Requirements ........ 6

Data Classification Guidelines ........ 7

Examples of Sensitive/Confidential Information ........ 7

Institutional Data ........ 7

Clinical/Research Data ........ 7

Personally Identifying Information ........ 7

Payment Card Data ........ 7

System Data ........ 7

Digital Media Types and Data Sanitization Methods ........ 8

Internal Disk Drives (ATA, SCSI) ........ 8

Removable Media ........ 9

Mobile Devices ........ 10

Other Office Equipment ........ 10

Software Recommendations for Formatting, Clearing and Purging ........ 10

Darik's Boot and Nuke (DBAN) ........ 10

Active@ Killdisk ........ 10

HDDErase (SecureErase) ........ 10

Hdparm ........ 10

Example of Sanitization Certificate ........ 11

McGill IT Asset Management Regulation ........ 11

Responsible Use Policy ........ 11

## Objectives

The following guidelines have been developed in support of McGill's Policy on the Responsible Use of McGill's IT Resources, and McGill's IT Asset Management Regulation.

http://www.mcgill.ca/secretariat/files/secretariat/responsible-use-of-mcgill-it-policy-on-the.pdf

http://www.mcgill.ca/procurement/files/procurement/mcgill_it-asset_reg.pdf

The Policy on the Responsible Use of McGill's IT Resources requires that McGill community members (faculty, staff and students) take all reasonable steps to protect the confidentiality, integrity, and availability of University data (i.e. information stored in or transmitted through McGill IT Resources, including documents, files, databases, e-mails and multimedia). The Policy also requires that McGill community members take the measures necessary to protect the security of McGill IT Resources and comply with University policies and procedures concerning data protection and records management.

McGill University's IT Asset Management Regulation prescribes the sound life-cycle management of the University's IT Assets. The Regulation clarifies the roles and responsibilities of McGill faculty and staff, as they are responsible for different steps along the life-cycle management of the University's IT Equipment.

The IT Asset Management Regulation identifies digital media sanitization (data-wiping) as an important component of IT Asset Management and requires that McGill faculty and staff abide by the following guidelines when managing University-related data.

In accordance with the aforementioned Policy and Regulation, the guidelines contained in this document specify:

1. The type of digital media that may require sanitization (Types of Digital Media)
2. The circumstances when digital media should be sanitized (Media Sanitization Requirements)
3. A data security classification scheme
4. Prescribed media sanitization methods

The respect of these guidelines will ensure that:

- There is no disclosure of credentials or data to unauthorized individuals or systems.
- Data that is of a private, proprietary or otherwise sensitive nature, including, but not limited to, Personal Information remains confidential.
- Embedded and removable storage media are properly sanitized before being redeployed at McGill or transferred for external reuse or recycling.
- Media Sanitization is recorded as part of the management of used or end-of-life media and IT equipment.

- Validation of data retention in relation to the data retention policy prior to sanitization. It is imperative to properly protect McGill data from destruction prior to expiry of the retention period.
- Validate that disposal is in accordance to any regulations, standards, policy, or legislation that may have jurisdiction on the data and/or equipment (e.g., McGill's IT Asset Management Regulation).

## Scope

These guidelines apply to all McGill community members identified as "Authorized Users" under McGill's Policy on the Responsible Use of IT Resources. This includes any McGill community member "who is an employee, student, alumni, appointee or other individual who has been granted permission, by virtue of the individual's role and responsibilities, to access certain data or systems that are part of McGill IT Resources."

## Related definitions (excerpts from the Policy on the Responsible Use of IT Resources)

Source: http://www.mcgill.ca/secretariat/files/secretariat/responsible-use-of-mcgill-it-policy-on-the.pdf

"Authorized User" is a member of the McGill University community who is an employee, student, alumni, appointee or other individual who has been granted permission, by virtue of the individual's role and responsibilities, to access certain data or systems that are part of McGill IT Resource

"Confidentiality" means the non-disclosure of Credentials or Data to unauthorized individuals or systems.

"Confidential Data" means Data that is of a private, proprietary or otherwise sensitive nature, including, but not limited to, Personal Information.

"Data" means information stored in or transmitted through McGill IT Resources, including documents, files, databases, e-mails and multimedia

"McGill IT Resources" means all Data, software, hardware, communications systems, storage systems, networks and devices connected to or making use of the University Network, regardless of who administers them.

## Media Sanitization Methods

The computing environment is constantly moving forward with new technologies. While there are numerous ways in which data is stored, the methods of disposing of the data can be classified into the following four processes:

**Format:** This is not considered as a sanitization method but it can be used for non-sensitive data. Format can be defined as the operating system functionality that erases all bookkeeping information on the disk and creates an internal address table that it later uses to locate information**.**

**Clear:** The use of hardware or software products to overwrite user accessible storage space with new values. Some devices do not support full overwrite but may only return the device to factory settings. This is not an example of clearing unless it is not possible to retrieve the cleared data.

**Purge:** The use of overwriting, block erase, Cryptographic Erase, through the use of dedicated, standardized device actions that apply media specific techniques to delete the data. Data should not be recoverable even using state of the art laboratory techniques. A note should be made about instant secure erase (ISE), it is a super-set of secure erase and utilizes encryption to make data unreadable. It is a method for cryptographic erase and this feature is offered by modern drives (specific models that came out after 2014).

**Destroy:** Physical destruction of the media in such a way that data cannot be recovered.

## 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:

| Ownership Change | **Data stored on Device** | Minimum Procedure |
|---|---|---|
| **Same Unit** | No Sensitive/Confidential Data | Format |
| **Different Unit** | No Sensitive/Confidential Data | Format |
| **Same Unit** | Sensitive/Confidential Data | Clear |
| **Different Unit** | Sensitive/Confidential Data | Clear |
| **External/Recycling/Dispose** | All Data | Purge/Destroy |
| **Non-Functioning Media** | All Data | Destroy |

- External legal or regulatory requirements for data sanitization with more stringent requirements will take precedence on McGill mandated media sanitization.
- A record of Sanitization must be completed for each media device
    - Internal form based on recommendations in Appendix G of NIST SP 800-88 Rev. 1 (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf)
    - Authenticated digital report/record of sanitized devices may be acceptable. (ex. Note in asset management/tracking system)
    - External media disposal services must also provide certificates of media sanitization/destruction.
- External providers of digital storage must provide assurance that media/data is properly sanitized as per McGill's guidelines.
- Records of sanitation must be kept on record for all sensitive and confidential data

# Data Classification Guidelines

Unless data stored on devices is clearly identified as non-sensitive/non-confidential, it should be treated as sensitive and /or confidential (i.e., confidential by default). An example of classification/categorization may be found in the NIST SP 800-60 "Guide for Mapping Types of Information and Information System to Security Categories" (http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol1-Rev1.pdf).

## Examples of Sensitive/Confidential Information

### Institutional Data

- Working documents regarding the internal operations at McGill
- Internal McGill related financial information (account numbers, balances, etc.)

### Clinical/Research Data

- Data associated with research with emphasis on any data which may be proprietary or restricted
- Clinical data (medical) where it may be associated with a patient record.

### Personally Identifying Information

- Names
- Date of Birth
- Address
- Email Address
- Social Insurance Number (SIN)

### Payment Card Data

- Credit card data (Name, Number, Expiry date, CVE)
- Banking Card data (Name, Number, Expiry date, CVE)

### System Data

- System Usernames
- Password Hashes
- License Keys
- Applications
- Source Code
- Configuration information
- Etc.

# 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 on disk. To further exacerbate the issue, new technologies such as SSDs may reallocate sectors entirely making traditional block level overwriting ineffective.

- ATA Hard Drives (HDD)
    - Format: Using the operating system's own format functionality before re-installing.
    - 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 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.
- SCSI Hard Drives
    - Format: Using the operating system own format functionality before re-installing.
    - 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 should be performed via the SCSI Sanitize Command. If unavailable, the media must be overwritten with multiple passes of a certified pattern (DoD Short, DoD 5220.22-M, RCMP TSSIT OPS-II, Gutmann Wipe) must be performed.
    - Destroy: Destruction/disposal of the media must be performed by a certified disposal company. A certificate of destruction must be provided.
- ATA Solid State Drives (SSD)
    - Format: Using the operating system own format functionality before re-installing.
    - 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. Due to sector remapping, special care must be taken to ensure that data is properly entirely cleared. Due to efficacy of secure erase, it is recommended with Solid State Drives to purge the media instead.

    - 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 be performed via the ATA Sanitize command,  ATA Secure Erase command or with Instant Secure Erase (if available) via the native interface (not through the enclosure). Validation of the clearing of data must be performed to ensure proper purging. Note that it may not be possible to use the drive in the original enclosure after a purge.
    - Destroy: Destruction/disposal of the media must be performed by a certified disposal company.  A certificate of destruction must be provided.
- USB Drives/Flash Memory/Memory Cards
    - 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: These devices do not normally support a sanitize function and will be device specific.  If not supported, device must be destroyed.
    - Destroy: Destruction/disposal of the media must be performed by a certified disposal company.  A certificate of destruction must be provided.
- Optical Media: CD, DVD, BD media
    - Destroy: All optical media must be physically destroyed (refer to cross cut-shred??)
- Legacy Magnetic Material (Tape/Floppy)
    - 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. Tapes may require “re-recording” with a safe signal. Multiple passes with more complex values may be used to further ensure proper clearing of the data.

- Purge: Degaussing with a certified degaussing device may be effective, however this may render the device unusable (unable to validate erasure) via normal means.
- Destroy: Destruction/disposal of the media must be performed by a certified disposal company. A certificate of destruction must be provided.

## Mobile Devices

When dealing with mobile devices it is important to note all areas where data can be stored. Data could be stored in the internal memory of the device, on removable media (microSD, etc.) or even the SIM card. It is also important to note that clearing/purging of the device will be highly device dependent.

- Internal Memory
  - Clear/Purge: Clearing/Purging of the internal memory of the device can be done via the device menu. The level of sanitization will be highly device dependent and should be validated.
  - Destroy: Destruction/disposal of the media must be performed by McGill's contracted certified recycling company.. A certificate of destruction must be provided.
- Phone SIM Cards
  - Clear: Clearing of the SIM Card of the device can be done via the device menu.
  - Purging: N/A See Destruction.
  - Destroy: Destruction/disposal of the media must be performed by a certified disposal company. A certificate of destruction must be provided.
- Removable Media
  - Refer to section regarding "USB Drives/Flash Memory/Memory Cards"

## Other Office Equipment

It is often overlooked that standard office equipment may have data storage. This could include:

- Printers and multifunction printer
- Photocopiers
- Fax (facsimile) machine
- Networking Devices (switches, routers)
- Etc.

## Software Recommendations for Formatting, Clearing and Purging

### Darik's Boot and Nuke (DBAN)

http://www.dban.org/

### Active@ Killdisk

http://www.killdisk.com/

### HDDErase (SecureErase)

http://cmrr.ucsd.edu/people/Hughes/secure-erase.html

### Hdparm

https://ata.wiki.kernel.org/index.php/ATA_Secure_Erase

## 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: | Backup Location: |
| Sanitization Details | |
| Method Type: ☐ Clear ☐ Purge ☐ Destroy | |
| Method Used: | |
| Method Details: | |
| Tools Used (including version): | |
| Verification Method: | |
| Notes: | |
| Media Destination | |
| Destination: ☐ Internal Reuse ☐ External Reuse/Recycling ☐ Disposal/Destruction ☐ Other | |
| Details: | |
| Signature | |
| I attest that the information provided on this statement is accurate to the best of my knowledge: | |
| Signature: | Date |
| Validation | |
| Name: | Department: |
| Email: | Phone: |
| Signature: | Date |

# Related McGill Policies and Regulations

### McGill IT Asset Management Regulation

McGill has published a regulation covering the life-cycle management of IT Equipment, which covers reuse and/or disposal of IT Equipment owned by McGill University. The current copy can be found at: http://www.mcgill.ca/procurement/files/procurement/mcgill_it-asset_reg.pdf

## Responsible Use Policy

In order to ensure that the McGill community handles data and other IT resources in a responsible manner, the *Policy on the Responsible Use of McGill Information Technology Resources* outlines the requirements that authorized users should adhere to. In particular, while not explicitly mentioned, the safe disposal of media is covered.

English: http://www.mcgill.ca/secretariat/files/secretariat/responsible-use-of-mcgill-it-policy-on-the.pdf

Français: http://www.mcgill.ca/secretariat/files/secretariat/responsible-use-of-mcgill-it-policy-on-the-french.pdf