Michigan Technological University
Information Technology

Data Sanitization Standard

Purpose

The purpose of this standard is to provide instructions on proper sanitization of data in both electronic and paper form. This standard also provides instruction on secure disposal of electronic storage media.

Scope

This standard applies to any electronic information storage or paper-based media containing sensitive or confidential data repurposed or transferred outside of Michigan Tech. This standard also applies to all University personnel who are responsible for the sanitization of potentially sensitive information and/or the disposal of electronic storage media.

Definitions

The National Institute of Standards and Technology (NIST) has defined four methods of data sanitization. These four methods are as follows:

- Disposal is defined as the act of discarding media with no other sanitization considerations. Examples of Disposal include discarding paper in a recycling container, deleting electronic documents using standard file deletion methods and discarding electronic storage media in a standard trash receptacle.
- Clearing is defined as a level of sanitization that renders media unreadable through normal means. Clearing is typically accomplished through an overwriting process that replaces actual data with 0's or random characters. Clearing prevents data from being recovered using standard disk and file recovery utilities.
- Purging is defined as a more advanced level of sanitization that renders media unreadable even through an advanced laboratory attack. In traditional thinking, Purging consists of using specialized utilities that repeatedly overwrite data; however, with advancements in electronic storage media, the definitions of Clearing and Purging are converging. For example, purging a hard drive manufactured after 2001 only requires a single overwrite. For the purpose of this Guideline, Clearing and Purging will be considered the same. Degaussing is also an acceptable method of purging electronic storage media; however, this typically renders the media unusable in the future.
- Destroying is defined as rendering media unusable. Destruction techniques include but are not limited to disintegration, incineration, pulverizing, shredding and melting. This is a common sanitization method for single-write storage media such as a CD or DVD for which other sanitization methods would be ineffective. This is also a common practice when permanently discarding hard drives.
- Electronic Storage Media is defined as any electronic device that can be used to store data. This includes but is not limited to internal and external hard drives, CDs, DVDs, Floppy Disks, USB drives, ZIP disks, magnetic tapes and SD cards.
- Non-public Information is defined as any information that is classified as Confidential (Tier I) or Internal/Private (Tier II) according to the Information Security Plan.

Regulatory Requirements

The Family Educational Rights and Privacy Act (FERPA), the Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and Payment Card Industry Data Security Standards (PCI DSS) require formal documentation of disposal procedures to ensure specific types of information is properly sanitized prior to being discarded.

Guidelines

The following are recommendations for when data sanitization should occur:

- All paper-based media should be disposed of when it is no longer necessary for business use, provided that the disposal does not conflict with University data retention policies or any regulatory requirements. Questions about retention requirements should be directed toward the appropriate data owner.
- All electronic storage media should be sanitized when it is no longer necessary for business use, provided that the sanitization does not conflict with University data retention policies, or any regulatory requirements. Questions about retention requirements should be directed toward the appropriate data owner.
- All electronic storage media should be sanitized prior to sale, donation or transfer of ownership. A transfer of ownership may include transitioning media to someone in your department with a different role, relinquishing media to another department, or replacing media as part of a lease agreement.
- The following are recommended for sanitization and disposal of paper-based media:
- Cross shredding should be used for Clearing and Purging of paper-based media.
- A third-party document destruction services should be leveraged for destroying paper-based media. A Certificate of Destruction should be requested, as evidence that documents were destroyed, and retained for future reference.
- The following are recommended for sanitization and disposal of Electronic Storage Media:
- Cross shredding should be used for destroying non-writeable CDs, DVDs and floppy disks.
- In situations where a third-party warranty or repair contract prevents proper sanitization of Electronic Storage Media, IT should be contacted for further guidance.

Data Removal and Destruction Management

It is important to maintain an effective method of managing the process of data destruction. This ensures that all media requiring cleaning or destruction is correctly organized and properly audited. Please contact IT for further instruction.

A record of all destruction/disposal of all sensitive data should be retained permanently. The log should contain a section for destruction or removal certificates; these provide evidence guaranteeing the destruction or sanitization of the media and the date on which the destruction occurred.

END OF DOCUMENT
Rev 9/20/16