Michigan Technological University
Information Technology

Media Destruction Procedure

Purpose

The purpose of this document is to provide a step-by-step solution for Michigan Tech's media destruction process. IT will provide the appropriate actions required to properly dispose of magnetic data storage devices and other media to ensure sensitive material cannot be recovered by an unauthorized individual. The procedures are an attempt to help individuals meet the requirements found in Michigan Tech's Data Sanitization Guideline.

Information systems capture, process, and store information using a wide variety of media. This information is located not only on the intended storage media but also on devices used to create, process, or transmit this information. Properly sanitizing media is a key element in assuring data confidentiality and reducing the risk or unauthorized disclosure of information. Protecting personally identifiable information includes but is not limited to student records, personnel records, and protected health and credit card information. In order to provide appropriate controls on the information we are responsible for safeguarding, we must properly dispose of media in all forms.

Scope

This Procedure applies to employees, contractors, consultants, temporary employees, and other workers at Michigan Tech. This document aids in establishing clear guidelines for media disposal/sanitization.

Definitions

Please see Data Sanitization Guidelines for reference.

NIST Guidelines

This Procedure has been adapted from Michigan Tech's Data Sanitization Guideline and from the National Institute of Standards and Technology (NIST) Special Publication 800-88 Guidelines for Media Sanitization. The information and recommendations made in this document have drawn heavily on the guidelines set forth by the NIST publication.

This adaptation has been developed for internal use. The intent of this document is to provide a simplified and tailored approach to manage and implement the NIST guideline within Michigan Tech.

Information Protection and Media Disposition

In order for Michigan Tech to have appropriate controls on the information it is responsible for safeguarding, it must properly protect all media used. An often rich source of illicit information collection is obtained as a result of dumpster diving for improperly disposed hard copy media or reconstruction of data on media not sanitized in an appropriate manner. Media flows in and out of an organization's control through recycle bins in paper form, out to vendors for equipment repairs, swapped into other systems due to upgrades or emergencies. This potential vulnerability can be mitigated through proper understanding of where information is located, what that information is and how to protect it.

Primary Media Types

Hard Copy

Hard copy media is physical representations of information. Paper printouts, printer, and facsimile ribbons are all examples of hard copy media. These types of media are often the most uncontrolled. Information tossed into the recycle bins and trash containers exposes a significant vulnerability to “dumpster divers” and overcurious employees, risking accidental disclosures.

Electronic (or soft copy)

Electronic media is the information contained in hard drives, USB removable media, disks, memory devices, phones, mobile computing devices, networking equipment, and many other types.

Media will continue to advance and evolve over time. The processes described in this document should guide media sanitization decision-making, regardless of the type of media in use.

Sanitization

Several different methods can be used to sanitize media. Four of the most common media types are presented in this section. Individuals should assess the media to be disposed of and determine the future plans for the media.

Level 1 Confidential Data—This pertains to the most classified information. Personal information, student records, credit card information, financial data all fall under the tier 1 security and should be handled with extreme care.

Level 2 Internal/Private Data—This information may contain private or restricted information. Information that is unique to an individual department.

Level 3 Public Data—Public and general information is considered to be a lower security.

For further explanation on Michigan Tech's levels of data, please see the Institutional Data Classification and Handling Policy.

Remember all media no matter the classification should be considered valuable information and should not be handled lightly. If uncertain on what type of data (confidential, internal/private, or public) exists on media please treat it as confidential or if you have any other questions, please call IT.

Steps for Media Sanitization

Between the time the media containing University sensitive data is removed from service, and the time it is sanitized or destroyed, it must be safeguarded. To facilitate secure sanitization of electronic media, Michigan Tech provides a secure drop box service in the basement of the EERC building just down from the elevators. Employees can bring digital media to this area for secure disposal however proper procedures must be followed for regulatory and compliance reasons.

Prior to transferring media over to IT for destruction, users must ensure:

- Management approval of the removal and destruction of media (if applicable)
- Information found on media is expired. (Media does not need to be archived for business or legal reasons)
- All information is wiped to the best of your ability. (Even if data is deleted the information still remains in some form and is possible to be recovered.)

IT has implemented a ticketing system (Service Desk) to aid in the sanitization and destruction process. Upon removal of media, a Service Desk ticket request needs to be completed by the employee. When creating the ticket please make sure to select IT Business Operations as the Service Team and Media Destruction as the Service. Your ticket will automatically be set to a status of “registered for destruction."

Once the ticket has been created, the relevant Footprints ticket number needs to be physically written on the media and delivered to IT within one business day. If media contains Level 1 data, media must be delivered within one hour of Footprints ticket creation.

To ensure notification of media within secure drop box, please raise the flag on the side of the box. Once the media is physically in IT's possession, the Footprints ticket status will be updated to "Media Destruction - IT Inventoried" and will be placed in a new secure location until it is shipped. You will receive notification via Footprints upon shipment and final destruction of media.

END OF DOCUMENT
Rev 9/20/16