

[Insert Company Name and Logo]	
Title: Media Sanitation & Disposal	P&P #:
Approval Date:	Review:
Effective Date:	Security Team

Purpose: This policy has been created to effectively destroy media while adhering to all known Security regulations.

Scope: This policy governs all electronic media and applies to all employees or other workforce members (whether paid, volunteer or contractor) using electronic media in all facilities under the organization's ownership.

Definitions:

1. Sensitive and regulated data: individually identifiable information that is transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium.
2. Securely Overwritten: The process of overwriting data with 1 and 0 to render the data irretrievable.
3. Physically Destroyed: The process of physically destroying electronic media to an extent where data is no longer retrievable.
4. Reuse of Hardware: The process of reallocating hardware that contains or may have contained sensitive and regulated data to an individual that does not have authority to access said data.
5. Degauss: Using a magnetic field to erase (neutralize) the data stored on magnetic media.
6. Sanitization: Removal or the act of overwriting data to a point of preventing the recovery of the data on the device or media that is being sanitized. Sanitization is typically done before re-issuing a device or media, donating equipment that contained sensitive information or returning leased equipment to the lending company.

Policy:

[Insert Company name] requires that, prior to disposal or reuse of hardware or media that contains or previously contained sensitive or regulated data, data will be securely overwritten or the device and/or media be physically destroyed and that such steps taken will be documented.

Procedure:

1. All electronic media must be properly sanitized before it is transferred from the current owner. The proper sanitization method depends on the type of media and the intended disposition of the media. This means that all sensitive or regulated data on decommissioned devices and storage media must be irretrievably destroyed, to protect the confidentiality of the data contained.

- a. If the device or media contains sensitive or regulated data that is not required or needed, and is not a unique copy, a data destruction tool must be used to destroy the data on the device or media prior to disposal. A typical reformat is not sufficient as it does not overwrite the data.
 - b. If the device or media contains the only copy of sensitive or regulated data that is required or needed, a retrievable copy of said data must be made prior to disposal.
2. All destruction/disposal of sensitive media will be done in accordance with federal and state laws and regulations and pursuant to the organization's written retention policy/schedule.
3. Records involved in any open investigation, audit or litigation should not be destroyed/disposed of. If notification is received that any of the above situations have occurred or there is the potential for such, the record retention schedule shall be suspended for these records until such time as the situation has been resolved. If the records have been requested during a judicial or administrative hearing, a qualified protective order will be obtained to ensure that the records are returned to the organization or properly destroyed/disposed of by the requesting party.
4. Any media containing sensitive or regulated data should be destroyed/disposed of using a method that ensures the data cannot be recovered. The methods of destruction, disposal, and reuse should be reassessed periodically, based on current technology, accepted practices, and availability of timely and cost-effective destruction, disposal, and reuse technologies and services.
5. Before reuse of any recordable and erasable media, all data must be rendered inaccessible, cleaned, or scrubbed. Any equipment or storage media that contains confidential, critical, and/or private information will be erased by appropriate means or destroyed by the Security Officer or his/her appointed designee before the equipment/media is reused. Methods include:
 - a. Removable magnetic "disks" (floppies, ZIP disks, and the like) and magnetic tapes (reels, cartridges) can be "degaussed" by an appropriately-sized-and-powered degausser or physically destroyed.
 - b. Fixed internal magnetic storage (such as computer hard drives), as well as removable storage, can be cleansed by a re-writing process. Software is used to overwrite all the usable storage locations of a medium. The simplest method is a single overwrite; additional security is provided by multiple overwrites with variations of all 0s, all 1s, complements (opposite of recorded character), and/or random characters.
 - c. A few kinds of "write-many" optical media (such as CD-RWs) can be processed via an overwrite method. This is not the case for the vast majority of "write-once" optical media in use (notably the CD-R). Write-once media cannot be degaussed, because such media are optical rather than magnetic. Therefore, only physical destruction will do.

- d. Removable "solid state" storage devices are also now available. These "flash memory" devices are solid state and are non-volatile (the memory maintains data even after all power sources have been disconnected). Examples include CompactFlash, Memory Stick, Secure Digital, Smart Media and other types of plug-ins, and a range of "mini-" and "micro-drive" flash devices that use USB or FireWire ports. Secure overwrites (following manufacturer specifications) are possible for these media as well. Neither degaussing nor over-writing offers absolute guarantees. However, complete destruction is available.
6. All original confidential, sensitive, and regulated data must be backed up on a regular basis. Backup mechanisms will be tested regularly to verify that the data can be efficiently retrieved. This includes backup of portable devices such as laptops and PDAs, when storing original sensitive and regulated data. Backups of original confidential, sensitive, and regulated data must be stored off-site in a physically secure facility.
7. Copies of documents and images that contain sensitive and regulated data and are not originals that do not require retention based on retention policies (e.g., provider copies, schedule print outs etc.) shall be destroyed/disposed of by shredding or other acceptable manner as outlined in this policy. Certification of destruction is not required.
8. Records scheduled for destruction/disposal should be secured against unauthorized or inappropriate access until the destruction/disposal of data is complete.
9. A record of all confidential, sensitive, and regulated data media sanitization should be made and retained by the organization. The organization has the responsibility to retain the burden of proof for any media destruction regardless of whether destruction is done by the organization or by a contractor. Retention is required because the records of destruction/disposal may become necessary to demonstrate that the confidential data was destroyed/disposed of in the regular course of business. Records of destruction/disposal, such as a certificate of destruction, should include:
 - a. Date of destruction/disposal.
 - b. Method of destruction/disposal.
 - c. Description of the destroyed/disposed record series or medium.
 - d. Inclusive dates covered.
 - e. A statement that the sensitive and regulated data was destroyed/disposed of in the normal course of business.
 - f. The signatures of the individuals supervising and witnessing the destruction/disposal.
10. If destruction/disposal services are contracted, the contract must provide that the organization's business associate will establish the permitted and required uses and disclosures of information by the business associate as set forth in the federal and state law. Agreements with business associates/vendors should also set minimum acceptable standards for the sanitization of media containing regulated data. The agreement or contract should:
 - a. Specify the method of data destruction/disposal.

- b. Specify the time that will elapse between acquisition and destruction/disposal of data/media.
- c. Establish safeguards against unauthorized disclosures of regulated data.
- d. Indemnify the organization from loss due to unauthorized disclosure.
- e. Require that the business associate/vendor always maintain liability insurance in specified amounts the contract is in effect.
- f. Provide proof of destruction/disposal (e.g., certificate of destruction).

VIOLATIONS:

Any individual found to have violated this policy, may be subject to disciplinary action up to and including termination of employment.

Attachments: None

Related Policies:

Data Retention Policy

Reference: NIST SP800-171.3.8.3

This template is provided by the Purdue University
Cyber Technical Assistance Program.

This template may be used, distributed, and shared
without restriction. The watermark may be removed
or replaced. White labeling this template is permitted.

For questions contact us via our website:

<https://cyber.tap.purdue.edu>