
# Dallas County Information Technology
# Data Disposal and Sanitization Policy

# 1. Scope

The Dallas County Data Disposal and Sanitization Policy applies to all County owned or leased electronic devices that contain a hard drive and any other device where County data may possibly be stored. This policy supersedes all other policies on this topic, either written or verbal.

# 2. Purpose

This document defines the policy necessary to ensure that Dallas County's deprecated or otherwise outdated computer, networking, or data storage hardware as well as other storage media ("Surplus Computing Devices"), and unneeded physical media comply with proper disposal and sanitization protocols. Broadly, exposure to the County from the loss of data privacy and security takes the form of:

- Unauthorized Release of Confidential Information such as Personally Identifiable (PII), Protected Health Information (PHI), or Criminal Justice Information System (CJIS) data.
- Unauthorized release of certain protected or confidential data that is required by the County to operate effectively.
- Violation of Software License Agreements - Most software is licensed for use on either a single computer system, to a single person, or to an organization. Typically, licenses are not transferable. Even when licenses are transferable, there are generally specific requirements that must be met to affect a transfer.

This Policy is designed to address proper disposal procedures for all Surplus Computing Devices. Such devices can be defined as computer hard drives, memory drives (e.g., M2 drives), data storage arrays, firmware chips, and any other hardware or solid-state device that may store County data in any form. All Confidential Information must be removed from County Surplus Computing Devices prior to their disposal. Proper sanitization and disposal procedures are key to ensuring data privacy and software license compliance. This Policy also addresses the proper destruction of unneeded physical media.

# 3. Policy

**Overview**

The transfer or disposition of Surplus Computing Devices and physical media shall be controlled and managed according to appropriate regulatory standards and guidelines. Data remains present on any type of storage device (whether fixed or removable) even after a disc is "formatted", power is removed, and the device is decommissioned. Simply deleting the data and formatting the disk does not prevent individuals from restoring data. Sanitization of the electronic media removes information in such a way that data recovery using common techniques or analysis is greatly reduced or prevented. Sanitization of physical media involves its physical destruction.

Various Dallas County departments and Elected Official's Offices regularly store Confidential Information or regulated information on computer hard drives and other forms of electronic media. As new equipment is obtained and older equipment and media reach End of Life, Confidential Information or regulated information on Surplus Computing Devices and media must be properly destroyed and otherwise made unreadable. Physical media that is no longer needed must be properly destroyed.

**Data Disposal Procedures**

All Surplus Computing Devices and portable electronic media must be processed through the Dallas County Office of Information Technology for proper disposal. Paper and hard copy records shall be disposed of in a secure manner as specified by Texas law and any other regulatory authority (e.g. FBI CJIS Security rules).

The Dallas County Chief Information Officer shall ensure procedures exist and are followed that:

(a) Address the evaluation and final disposition of Confidential Information, hardware, or electronic media regardless of media format or type.
(b) Consult with the respective Dallas County Law Enforcement Agencies, as appropriate, as to the disposal of their respective Surplus Computing Devices.
(c) Specify a process for making Confidential Information or regulated information unusable and inaccessible. These procedures should specify the use of technology (e.g., software, special hardware, etc.) or physical destruction mechanisms to ensure Confidential Information or regulated information is unusable, inaccessible, and unable to be reconstructed.
(d) Authorize personnel to dispose of Confidential Information or equipment as each situation dictates. Approved disposal methods include:
    (1) Physical Print Media shall be disposed of by one (or a combination) of the following methods:
        - Shredding - Physical Media shall be shredded using Dallas County's approved document shredding vendor and their respective shredding bins on Dallas County property. The approved Dallas County shredding vendor shall certify the periodic destruction of Physical Media to an approved representative of the Dallas County Sheriff's Department and the Chief Privacy Officer.
        - Shredding Bins - Disposal shall be performed using locked bins located on-site using Dallas County's approved shredding vendor by October 1, 2023.
        - Incineration – Physical Print Media maybe physically destroyed using licensed and bonded information disposal contractor.
    (2) Electronic Media (physical hard drives, tape cartridges, CDs, printer ribbons, memory drives, printer, and copier hard drives, etc.) shall be disposed of by one of the following methods:
        - Overwriting Magnetic Media - Overwriting uses a program that, at a minimum, adheres to the DoD 5220.22-M[1] overwrite standard to write binary data sector by sector onto the media that requires sanitization in the presence of a Dallas County authorized employee. After the conclusion of the overwriting, the IT Asset Manager, Chief Information Security Officer and the Chief Privacy Officer shall take a representative sampling of the electronic media overwritten to verify its effectiveness.
        - Degaussing - Degaussing consists of using strong magnets or electric degaussing equipment to magnetically scramble the data on a hard drive into an unrecoverable state. After the conclusion of the Degaussing process, the IT Asset Manager, the Chief Information Security Officer, and the Chief Privacy Officer

[1] https://www.jetico.com/blog/dod-522022-m-explained-data-erasure-standards#:~:text=These%20standards%20specify%20the%20overwrite,requires%203%20secure%20overwriting%20passes.

shall take a random sampling of the electronic media, so degaussed, to verify its effectiveness.

- Physical Destruction – meaning the complete destruction of electronic media by means of crushing, shredding, or disassembling the asset and ensuring no data can be extracted or recreated. The Physical Destruction of electronic media shall be done in the presence of the IT Asset Manager, Chief Information Security Officer, and the Chief Privacy Officer.

IT documentation, hardware, and storage media that have been used to process, store, or transmit Confidential Information, CJIS data, PHI, or PII shall not be released from Dallas County's possession until it has been sanitized and all stored information has been cleared using one of the above methods. Further, the IT Asset Manager, the Chief Information Security Officer, and the Chief Privacy Officer shall execute and keep a triple-signed record for individual electronic media notating which disposal method was utilized and the identifiers of each form of electronic media destroyed is accordance with NIST Special Publication 800-88, Revision 1, Section 4.8. The records required in this Section shall be maintained by the Chief Privacy Officer.

## 4. Periodic Reviews

This Policy will be reviewed and updated on an annual basis.

## 5. Enforcement and Exception Handling

This Policy applies to all County owned or leased electronic devices that contain a hard drive and any other device where County data may possibly be stored. All department heads and elected must comply with this Data Disposal and Sanitization Policy. Failure to comply with the Criminal Justice Information Policy (CJIS), or other applicable data privacy regulations, Dallas County Code, or this Policy can result in a loss of access and/or disciplinary actions, up to and including termination of employment, contracts and/or other relationships. Additionally legal action may also be taken in response to violations of applicable regulations and laws.

Requests for exceptions to Dallas County security policies should be submitted to the ServiceDesk and routed to the Security Team. Exceptions will be permitted only upon receipt of written approval from the Dallas County Chief Information Officer and the Chief Privacy Officer.

## 7. Revision History

| ***Date:*** | ***version #:*** | ***Description:*** | ***Updated by:*** |
|---|---|---|---|
| 06/02/2023 | 1.0 | Initial Draft | Kroll |
| 7/6/23 | 1.1 | Revised Draft | Randall Miller, CPO |
| 7/18/23 | 1.2 | Revised Draft | Randall Miller, CPO |