

# Securely Wiping Unclassified Information In U.S. Federal Agencies

The National Archives and Records Administration (NARA) is responsible for developing information security standards and guidelines for unclassified information. The guidelines in 32 CFR Part 2002 were developed in collaboration with government agencies to improve the 'patchwork' of policies covering the handling and management of unclassified data.

The guidelines cover the storage, safeguarding, access, dissemination, decontrolling, marking and destruction of this data. These policies are to be implemented by appropriate personnel and are under the oversight of the Information Security Oversight Office (ISOO) of the NARA.

## Disposal

The destruction of unclassified data may be destroyed when it is no longer needed by the agency and permitted by the NARA records disposition schedule. This schedule covers the length of time a document needs to be stored by an agency to comply with the Freedom of Information Act and other regulations.

When destroying unclassified information agencies must make the data "unreadable, indecipherable and irrecoverable". What method the agency uses to have the information reach this state is mandated their internal policy. If the agency does not have an internal policy then they must destroy data as recommended by NIST 800-53 / NIST 800-88 or 32 CFR 2001.47.



NIST 800-53 and 800-88 recommend media sanitization techniques for electronic information that include clearing, purging, cryptographic erase, de-identification of personally identifiable information, and destruction. Organizations should determine their level of sanitization depending on the data's significance and consequence of a data breach. Data software tools, like WipeDrive, perform clearing, purging and cryptographic erasure and provide certificates of destruction for future audits.

The 32 CFR 2001.47 requires non-electronic information to be destroyed with burning, cross-cut shredding, wet-pulping, melting, mutilation, chemical decomposition, or pulverizing.

## Quick Fact:

The **National Archives and Records Administration (NARA)** is an independent agency of the United States government charged with the preservation and documentation of government and historical records. It is also tasked with providing destruction protocols for US Federal Agencies.

## Implementation On Electronic Information

Each agency has created their own record retention policies. Unclassified information that is to be sanitized must comply with these policies. Federal entities should also track and document their actions. This can include listing personnel who reviewed and approved sanitization and disposal actions, types of media sanitized, files stored on the media, sanitization methods used, date and time of the sanitization actions, personnel who performed the sanitization, verification actions taken and personnel who performed the verification, and the disposal actions taken. Organizations must verify that the sanitization of the media was effective prior to disposal.

Complying with NARA regulations when managing unclassified data will ensure your organization sanitizes media correctly and reduce the vulnerability of a data breach. WipeDrive Enterprise is a proven software-based erasure tool that meets NARA 32 CFR Part 2002 requirements when sanitizing your media storage. Request a trial today or contact our Sales Team at [801.224.8900](tel:8012248900).

