ADMINISTRATIVE MEMORANDUM
COUNTY OF SAN MATEO

NUMBER: F-1

SUBJECT: Destruction of Confidential Documents

RESPONSIBLE DEPARTMENT: Information Services Department (ISD)

APPROVED: _____ **DATE:** November 7, 2018
Michael P. Callagy, County Manager

This memorandum replaces an earlier version of Memorandum F-1 dated March 28, 1997 which pertained to the destruction of confidential documents. This memorandum revises and expands the policy to cover documents in electronic/digital format.

1. **Purpose**
   This policy outlines the proper methods of destroying confidential documents that are either in paper or electronic format. The purpose of this policy is to ensure that the disposal of all confidential records, in all formats including digital data, is made by appropriate means that would render the information without the risk of being recovered. Confidential documents are any documents that contain sensitive information, are classified as personally identifiable information (PII), or that contain Protected Health Information (PHI) pursuant to the Health Insurance Portability and Accountability Act (HIPAA).

2. **Scope**
   This policy applies to all departments. Employees, contractors, vendors, interns, extra-help, and any party who provides services or work for the County will be collectively known as "workforce members" for purposes of this document and shall be familiar with the destruction of confidential documents.

3. **Policy**
   A. General Information:
      - Destruction of any documents involved in an open investigation, audit, or litigation shall not be permitted.
      - Documents may appear in forms that include, but are not limited to, paper documents, email, electronic format stored on hard drives, shared drives, removable medias, and/or in the Cloud.
      - Destruction of any confidential documents shall be timely and comport with the retention guidelines set forth in the County's Document Retention Policy. The individual department may also have specific guidelines regarding document retention that must be followed.

- Destruction of confidential documents shall be authorized by the Department Head or his or her designee.

B. Paper-based documents
   - Confidential documents shall not be disposed of in the garbage without shredding or obliteration, meaning that all paper-based documents must be destroyed in a manner that would be impossible to reconstruct and to read the information.
     - Acceptable methods include shredding, incineration, and pulverization.
   - Documents awaiting destruction shall be housed in a secured collection container.
     - If a third party is used a secure chain of custody protocol must be employed and a certificate of destruction must be provided to ensure documents were securely destroyed within 24 hours.

C. Electronic/digital-based documents
   - The deletion of electronic/digital-based documents is not the same as destruction. All electronic media must be destroyed (i.e. the media would render the information without the risk of being recovered).
   - All confidential County information on decommissioned devices and electronic storage media must be irretrievably destroyed to protect the confidentiality of the data. Any question regarding appropriate destruction methods should be referred to the CIO or his/her designee. Acceptable destruction practices include, but are not limited to the following protocols:
     - Removable magnetic disks and tapes shall be degaussed or crushed with a destruction tool, which shall be provided by the Information Services Department (ISD), to destroy the data on magnetic storage device or media prior to its disposal.
     - Fixed and removable computer hard drives can either be sanitized with an overwrite command or through the use of tools as authorized and/or provided by the CIO or his/her designee, such as a degausser or crusher.
     - Media that are not affected by tools (i.e., degausser or crusher) such as compact discs, memory sticks or USB drives, solid state drives, and any media that cannot fit into the degausser or crusher shall be properly destroyed by an outside professional service.
     - Hardware shall be properly disposed of when no longer used in accordance with County Surplus Property Procedures detailed in Ordinance 2.92.120; however, no re-constructible residual representation of the data may be stored on the hardware.
     - Before any confidential data is removed from any electronic storage media, the individual department will verify that all documents

required to be retained has been moved to an appropriate storage medium.

4. Revision History

Effective Date	Changes Made
March 28, 1997	Policy established
November 7, 2018	Policy updated