SACRAMENTO COUNTY	**Policy #TBD**
Subject: Data Classification and Retention	
Responsible Department: Technology	
Effective Date: 6/17/2024	
DocuSigned by: David Villanueva DF677889D344455...	
David Villanueva **County Executive**	
DocuSigned by: Sylvester Fadal ECCA59D0AF44478...	
Sylvester Fadal **Deputy County Executive**	
DocuSigned by: Rami Zakaria 114051389255458...	
Rami Zakaria **Chief Information Officer**	

1. Purpose

This policy identifies the authority within the County of Sacramento ("the County") responsible for data classification and retention; defines County data classifications; and specifies how long data should be retained.

.

2. Authority

Chief Information Officer.

3. Scope

This policy applies to all County data and all County departments reporting to the County Executive

4. Policy

4.1 Responsibility

a. Department Directors have the authority to manage and classify data according to the definitions below; to identify whether data contains personal and/or sensitive information; and to allow data to be deleted when its retention is neither necessary nor required by law.

b. Department Directors are responsible for defining precautions to ensure the security of and appropriate access to each data classification, and for working with the Department of Technology to confirm that these precautions are followed.

4.2 Data Classifications

General Rule

a. The County shall identify data according to the classifications defined in 4.3, 4.4, and 4.5 below. Data shall be classified as "Internal" unless (a.) it is published as "Public," such as information on the County website, or (b.) it specifically meets the definition of "Confidential" below.

b. Labeling documents is intrinsic to the County's data management and information security programs. Documents shall be labeled according to the definitions below and the specific guidance in Section 4.6 below.

4.3 Public Data

Public data (use the label "Public") is freely available and accessible to the public without any restrictions. With respect to County information and data, the presumption will be in favor of openness to the extent permitted by the law, subject to valid privacy, confidentiality, security, or other restrictions and exceptions afforded under the law.

Examples of Public data (non-exclusive list):

a. County-published press releases, reports, and website posts

b. Basic Parcel Information (Situs address, Tax Rate Area Code, Lot Size, etc…)

c. County Bid/Contract/RFP listings

4.4 Internal Data

Internal data (use the label "Internal") is not meant for public disclosure OR not to be made publicly available without formal review, as in the case of a Public Records Act request.

Internal data is created or bestowed upon the organization by Business Partners, customers, and/or workforce members. Internal data needs to be secured to protect organizational interests as well as to ensure continued stakeholder trust.

Examples of Internal data (non-exclusive list):

a. Customer communications

b. Organizational email not containing Confidential data

c. Standards and Procedures

d. Organizational planning and strategy documents

e. Intranet information and information generally kept on internal file shares

4.5 Confidential Data

Confidential data (use the label "Confidential") is information maintained by County departments that are either:

a. Exempt from disclosure under the provisions of California Public Records Act (CPRA) section 7920 et. seq.; or

b. Protected from disclosure by law.

4.5.1 Examples of Confidential data exempt from disclosure under CPRA (non-exclusive list):

a. Personnel, medical, or similar files the disclosure of which would constitute an unwarranted invasion of personal privacy.

b. Preliminary drafts, notes, or interagency or intra-agency memoranda that are not retained by the public agency in the ordinary course of business.

c. Records pertaining to pending litigation to which the public agency is a party, or to claims made pursuant to California Code Division 3.6 (commencing with Section 810), until the pending litigation or claim has been finally adjudicated or otherwise settled.

d. Geological and geophysical data, plant production data, trade secret data and similar information relating to utility systems development, or market or crop reports, that are obtained in confidence from any person.

4.5.2 Examples of Confidential data whose protection and nondisclosure are required by law (nonexclusive list):

a. Personally Identifiable Information (PII) protected data, per 2 CFR § 200.1, consists of any data that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.

b. Criminal Justice Information (CJI) protected information consists of all private or sensitive information gathered by local, state or Federal law enforcement agencies. CJI is protected by 28 U.S.C. § 534 and a variety of other Federal and California statutes and regulations.

c. Federal Tax Information (FTI) protected data consists of any return or return information received from the Internal Revenue Service or any secondary source that is protected by the confidentiality provisions of Internal Revenue Code § 6103.

d. Health Insurance Portability and Accountability Act (HIPAA) per 45 CFR Part 160, Part 162 and Part 164 protected data consists of any identifiable health information that is used, maintained, stored, or transmitted by a HIPAA-covered entity or business associate in relation to the provision of healthcare or payment for healthcare services.

e. Payment Card Industry Data Security Standard (PCI DSS) data that are protected through adherence to the PCI Security Standards, including both payment card and cardholder personal information.

4.6 <u>Labeling Documents with Data Classification</u>

<u>General Rule</u>

Classification labels shall be used to summarize the classification of Public, Internal and Confidential data in a document as noted in the data classification definitions above. County documents should <u>always</u> be labeled with the document's data classification if possible.

4.6.1 <u>Automatic Labeling</u>

Data Classification labels will be automatically applied when possible. Automatic labeling will be based on document analysis and applied when the document is saved. If automatic labeling isn't possible, manual labeling will be required.

4.6.2 <u>Manual Labeling</u>

Manual labeling shall be performed by the document owner. It is done either by using the dropdown list of label categories in the M365 sensitivity bar or by manually inserting a document label into the footer of an unlabeled document.

Whenever possible, document owners shall use published labels for documents (e.g., Microsoft files, Adobe PDF files, etc.) or labels available within other County systems/applications.

4.7 Data Retention

Data sets maintained by the County will be retained (a.) until the longest retention period specified by law or policy, or (b.) if there is no specified retention period, data is retained until it is determined that the data is no longer needed for administrative, legal, audit, or other purposes.

5. **Review**: Triannual

6. **References**

- California Statewide Information Management Manual (SIMM) § 5305-A
- California Public Records Act (CPRA), California Government Code § 7920 et seq.
- 28 U.S.C. 534 (CJI data protection)
- Internal Revenue Code § 6103 (FTI data protection).
- Confidentiality of Medical Information Act, California Civil Code § 56 et seq.
- Patient Access to Health Records Act, California Health and Safety Code § 123100-123149.5
- Health Insurance Portability and Accountability Act (HIPAA) Regulations, 45 C.F. R.
- § 160 and 164
- California Consumer Privacy Act (CCPA), § 1798 et seq.
- PCI Security Standards