

**COUNTY OF SAN DIEGO  
ADMINISTRATIVE MANUAL**

---

SUBJECT: COUNTY DATA/INFORMATION – CLASSIFICATION,  
PROTECTION LEVEL, AND PROPER SECURITY

ITEM  
NUMBER **0040-09-02**

EFFECTIVE DATE: JUNE 5, 2008

PAGE 1 of 10

---

**I. PURPOSE**

This policy defines the classification, protection level, and the proper security and handling of County data/information as it is created, received, stored, deleted, disposed of, or transmitted in all formats.

**II. BACKGROUND**

County data/information is a valuable business asset. There are many different types of County data/information requiring a range of security, protection and handling protocols.

The County has developed data classification guidelines to assist in determining the security, protection and handling protocol for the different types of County data/information. The data/information is classified based on its sensitivity (e.g. confidential, sensitive, public). Federal and State laws and regulations also determine the classification of County data/information. The Data Classification Guidelines also serve to establish a standard method of handling similar County data/information consistently across the County.

Once the data/information is classified, the proper security controls are then determined. Separate and apart from legal classifications, a County appointed information owner may require additional or special authorization for County data/information because of its value and sensitivity. Some data/information may have a higher sensitivity to loss or disclosure and/or have an adverse impact to the County if improperly safeguarded, misused, mismanaged or disclosed without proper authorization.

The County guideline extends to all formats of handling data/information. Examples include, but are not limited to, verbal communication, paper/documents, electronic information, the physical location and storage of the data, or carrying it on mobile devices (e.g. Laptop, PDA, Blackberries).

The County has established policies and procedures to protect the integrity, security and confidentiality of County data/information. Departmental procedures may increase the security controls as needed. In the performance of regular duties and assignments, authorized users must be familiar with and observe the policies and procedures governing County data/information.

**III. SCOPE**

This Administrative Manual section and the policies herein apply to all departments, offices of the County and other authorized users.

**COUNTY OF SAN DIEGO  
ADMINISTRATIVE MANUAL**

---

SUBJECT: COUNTY DATA/INFORMATION – CLASSIFICATION,  
PROTECTION LEVEL, AND PROPER SECURITY

ITEM  
NUMBER **0040-09-02**

EFFECTIVE DATE: JUNE 5, 2008

PAGE 2 of 10

---

**IV. POLICY**

**A. General Statements**

1. All County data/information shall be provided on a need-to-know basis to protect the information from unauthorized disclosure, damage, modification, or misuse. 'Need-to-know' is defined as granting access only to those files and programs that the authorized user needs in order to perform his/her assigned job functions.
2. Departmental procedures regarding data classification and security shall comply with applicable Federal and State laws that govern the privacy and confidentiality of data. Additionally, Departmental procedures may impose certain restrictions that may not be specifically covered by Federal or State law, or other regulations.
3. Consult with County Counsel or the County Privacy Officer for information regarding applicable confidentiality or privacy laws and regulations.
4. State and Federal laws and regulations provide that certain County data/information is confidential, privileged or publicly accessible. Those laws and regulations control over any County policy, guideline or individual decision concerning the classification or use of data/information.
5. All data/information residing in the County's information systems, regardless of its source, will be treated as County property for the purpose of monitoring, accessing, retrieving, restoring, deleting, protecting or disclosing such data/information.
6. All data/information belonging to third parties residing on the County's information systems shall be treated in the same manner as County data/information under this policy.
7. All authorized users of County data/information are to be provided adequate technical, physical or procedural controls to enable them to protect data/information that they access, create or use in connection with County business or programs.
8. County data/information shall be used responsibly and ethically. Personal use of the information is prohibited.
9. County data/information categorized as 'restricted', 'confidential', or 'sensitive' must reside within the security controls of County information systems. For County mobile devices such as laptops, PDAs,

**COUNTY OF SAN DIEGO  
ADMINISTRATIVE MANUAL**

---

SUBJECT: COUNTY DATA/INFORMATION – CLASSIFICATION,  
PROTECTION LEVEL, AND PROPER SECURITY

ITEM  
NUMBER **0040-09-02**

EFFECTIVE DATE: JUNE 5, 2008

PAGE 3 of 10

---

or Blackberries, the user is responsible for keeping the device safe and secured. The storage of this data/information in personally owned equipment is prohibited.

**10.** The County retains the right to monitor, access, retrieve, restore, delete or disclose County data/information and information systems, at any time without prior notice, to ensure policy compliance, except where specifically prohibited by law.

**B. Access to County Data/Information**

**1.** Prior to being authorized to access, create or use County data/information in the performance of their regular duties and assignments, all authorized users must sign a ***Summary of Policies Regarding County Data/information and Information Systems*** form by which they are given an understanding of their responsibilities for protecting County data/information and information systems according to the County's policies and departmental procedures.

**C. Data/Information Owner**

**1.** All County data/information is assigned to a specific department, office or agency with primary accountability for the data/information ("information owner").

**2.** The information owner is responsible for making decisions about the sensitivity and criticality of the information. The classification designated by the information owner will determine the certain way the information is to be handled and protected.

**D. Authorized User Responsibilities**

**1.** The authorized user shall comply with the proper handling and security requirements specified by the information owner.

**2.** Authorized users who need a certain type of access to data/information must have the owner's consent. Direct interaction with the information owner may not be necessary if access to the requested information is part of the user's profile to perform specific job functions and the information owner's consent has been previously obtained.

**3.** Authorized users shall be familiar with Federal or State confidentiality or privacy laws pertaining to data/information that they access, create or use in conducting their duties and assignments.

**COUNTY OF SAN DIEGO  
ADMINISTRATIVE MANUAL**

SUBJECT: COUNTY DATA/INFORMATION – CLASSIFICATION,  
PROTECTION LEVEL, AND PROPER SECURITY

ITEM  
NUMBER **0040-09-02**

EFFECTIVE DATE: JUNE 5, 2008

PAGE 4 of 10

**E. Representing Personal Opinions**

Authorized users shall not represent personal opinions as those of the County in any format unless specifically authorized to do so for the County.

**F. Reporting Suspicious Activity**

The integrity and security of County data/information depends on the observation of proper business practices by all authorized users.

All authorized users are requested to report any suspicious activity regarding data/information damage, misuse, unauthorized disclosure or modification to their manager/supervisor or their department's information security manager.

Examples: Suspicious activity may consist of, but not be limited to:

- Signs of unauthorized equipment usage
- Unidentifiable files found on file servers or in the home directory
- Paper containing 'Restricted', 'Confidential', or 'Sensitive' data/information found in recycle or trash receptacles without being shredded.
- Unusual activity recorded in log files
- Missing equipment (e.g. computer hard drive, laptop, PDA).
- Other unusual or unauthorized activities.

**G. Data Classification Guideline**

For the purpose of responsible management and control of County data/information, the following guidelines and tools are established to assist in classifying and protecting County data/information:

<b>TYPE</b>	<b>DESCRIPTION</b>	<b>EXAMPLE</b>	<b>SECURITY LEVEL</b>
RESTRICTED	This classification applies to the most sensitive business information. It is strictly for use within the County or by specific government agencies or business partners who have a legal right to the information. This information is considered critical to the County's ongoing operations  Viewing and use is intended only for one person or for very specific individuals.  Data/information in any format must never be	Passwords, Health Information, operation systems security controls	Highest Possible

**COUNTY OF SAN DIEGO  
ADMINISTRATIVE MANUAL**

SUBJECT: COUNTY DATA/INFORMATION – CLASSIFICATION,  
PROTECTION LEVEL, AND PROPER SECURITY

ITEM  
NUMBER **0040-09-02**

EFFECTIVE DATE: JUNE 5, 2008

PAGE 5 of 10

TYPE	DESCRIPTION	EXAMPLE	SECURITY LEVEL
	<p>shared with unauthorized persons, offices, or agencies.</p> <p>Its unauthorized disclosure could seriously and adversely impact the County, its operation, its business partners and/or it's customers.</p> <p>Such information must not be shared, copied or removed from the County's operational control without specific authority as applicable.</p> <p>Misuse or unauthorized disclosure of certain restricted information may result in Federal or State fines/penalties to the County.</p>		
CONFIDENTIAL	<p>This classification applies to less sensitive business information and is strictly for use within the County or by specific government agencies or business partners who have a legal right to the information. . This information is considered critical to the County's ongoing operations.</p> <p>Viewing and use is intended for a limited number of individuals.</p> <p>Data/information in any format must never be shared with unauthorized persons, offices, or agencies.</p> <p>Its unauthorized disclosure could adversely impact the County, its business partners and/or its customers.</p> <p>Such information must not be copied or removed from the County's operational control without specific authority.</p> <p>Misuse or unauthorized disclosure of certain confidential information may result in Federal or State fines/penalties to the County.</p>	attorney-client communications, patient medical records, Site Emergency Response plans	Very High
SENSITIVE	<p>This classification applies to information that is delicate in nature and is strictly for use within the County or by specific government agencies or business partners who have a legal right to the information. .</p> <p>Viewing and use is intended for a relatively wide body of authorized users.</p>	Employee personnel records, financial records and dollar transactions, research	HIGH

**COUNTY OF SAN DIEGO  
ADMINISTRATIVE MANUAL**

SUBJECT: COUNTY DATA/INFORMATION – CLASSIFICATION,  
PROTECTION LEVEL, AND PROPER SECURITY

ITEM  
NUMBER **0040-09-02**

EFFECTIVE DATE: JUNE 5, 2008

PAGE 6 of 10

TYPE	DESCRIPTION	EXAMPLE	SECURITY LEVEL
	<p>Data/information in any format must never be shared with unauthorized persons, offices or agencies.</p> <p>Its unauthorized disclosure could seriously and adversely impact the County and/or its employees.</p> <p>Such information must not be copied or removed from the County's operational control without specific authority.</p>	<p>projects, operational system data</p>	
UNCLASSIFIED	<p>This classification applies to all other information which does not clearly, fit into any of the above three classifications.</p> <p>Data/information in any format must never be shared with unauthorized persons, offices or agencies.</p> <p>While unauthorized disclosure is against policy, it is not expected to seriously or adversely impact the County, its employees, its business partners, and/or its customers.</p>	<p>Annual reports; Board letters; inventories</p>	Medium
INTERNAL USE	<p>This classification applies to normal operating information.</p> <p>Viewing and use is intended for employees only. It can be made available County wide or to specific employees in a group, department, office or business unit.</p> <p>Data/information in any format must never be shared with unauthorized persons, offices, or agencies.</p> <p>While unauthorized disclosure is against policy, it is not expected to seriously or adversely impact the County, and/or its employees.</p>	<p>Employee phone directory, memos, minutes of meetings, internal announcements, policy &amp; procedure manuals, internal project reports, County Intranet</p>	Medium
PUBLIC	<p>This classification applies to information that is approved for public release to the general community.</p> <p>Viewing and use is intended for distribution outside the County. This information may be freely disseminated.</p>	<p>County Web-site on the Internet, Job Announcements, press releases</p>	Low to none

**COUNTY OF SAN DIEGO  
ADMINISTRATIVE MANUAL**

SUBJECT: COUNTY DATA/INFORMATION – CLASSIFICATION, PROTECTION LEVEL, AND PROPER SECURITY

ITEM NUMBER **0040-09-02**

EFFECTIVE DATE: JUNE 5, 2008

PAGE 7 of 10

**H. Level of Protection**

The following table defines minimum security controls for data/information requiring a high level of protection. Apply as applicable. The references to “mark as...” means to include, on the “subject line” of the email, the terms indicated. Appointed Information Owners may develop more stringent controls in their procedures as is necessary.

<b>OPERATION</b>	<b>RESTRICTED</b>	<b>CONFIDENTIAL</b>	<b>SENSITIVE</b>
<b>VERBAL</b>	<ul style="list-style-type: none"> <li>Do not share with anyone</li> <li>Discuss privately</li> <li>Avoid being overheard over the telephone</li> </ul>	<ul style="list-style-type: none"> <li>Discuss with limited individuals</li> <li>Avoid being overheard over the telephone</li> </ul>	<ul style="list-style-type: none"> <li>Discuss within work area</li> </ul>
<b>EMAIL</b>	<p><i>Internal Email:</i></p> <ul style="list-style-type: none"> <li>Limit or prohibit if possible</li> <li>Include a disclosure clause</li> <li>Mark as ‘Private’</li> <li>Send only to specific employees</li> </ul> <p><i>External Email:</i></p> <ul style="list-style-type: none"> <li>Limit or prohibit if possible</li> <li>Do not send out unless encrypted.</li> <li>Include a disclosure clause</li> </ul>	<p><i>Internal Email:</i></p> <ul style="list-style-type: none"> <li>Limit</li> <li>Include a disclosure clause</li> <li>Mark as ‘Confidential’ or if an attorney-client communication – “Confidential: Attorney Client Communication”</li> <li>Send only to limited employees</li> </ul> <p><i>External Email:</i></p> <ul style="list-style-type: none"> <li>Do not send out unless encrypted.</li> <li>Include a disclosure clause</li> </ul>	<p><i>Internal Email:</i></p> <ul style="list-style-type: none"> <li>Limit</li> <li>Include a disclosure clause</li> <li>Mark as ‘Personal’</li> <li>Send only to a particular group of employees</li> </ul> <p><i>External Email:</i></p> <ul style="list-style-type: none"> <li>Do not send out unless encrypted.</li> <li>Include a disclosure clause.</li> </ul>
<b>FAX</b>	<ul style="list-style-type: none"> <li>Limit or prohibit if possible</li> <li>Cover sheet to include a disclosure clause</li> <li>Contact recipient prior to sending. Recipient must confirm receipt of fax.</li> </ul>	<ul style="list-style-type: none"> <li>Limit</li> <li>Contact recipient prior to sending. Recipient must confirm receipt of fax.</li> <li>Cover sheet to include a disclosure clause</li> </ul>	<ul style="list-style-type: none"> <li>Limit</li> <li>Contact recipient prior to sending. Recipient to confirm receipt of fax.</li> <li>Cover sheet to include a disclosure clause</li> </ul>
<b>INTERNET</b>	Encrypted only	Encrypted only	Encrypted only

**COUNTY OF SAN DIEGO  
ADMINISTRATIVE MANUAL**

SUBJECT: COUNTY DATA/INFORMATION – CLASSIFICATION,  
PROTECTION LEVEL, AND PROPER SECURITY

ITEM NUMBER **0040-09-02**

EFFECTIVE DATE: JUNE 5, 2008

PAGE 8 of 10

OPERATION	RESTRICTED	CONFIDENTIAL	SENSITIVE
INTER-OFFICE or EXTERNAL MAIL (PAPER)	<p><i>Inter-Office Mail:</i></p> <ul style="list-style-type: none"> <li>• Use double envelope.</li> <li>• Mark outside envelope with “To be opened by addressee only”</li> <li>• Recipient to confirm receipt</li> </ul> <p><i>External Mail:</i></p> <ul style="list-style-type: none"> <li>• Hand deliver</li> <li>• Use courier or registered mail</li> <li>• Mark outside envelope with “To be opened by addressee only”</li> <li>• Recipient to confirm receipt</li> </ul>	<p><i>Inter-Office Mail:</i></p> <ul style="list-style-type: none"> <li>• Use double envelope.</li> <li>• Mark outside envelope with “To be opened by addressee only”</li> <li>• Recipient to confirm receipt.</li> </ul> <p><i>External Mail:</i></p> <ul style="list-style-type: none"> <li>• Hand deliver</li> <li>• Use courier or registered mail</li> <li>• Mark outside envelope with “To be opened by addressee only”</li> <li>• Recipient to confirm receipt</li> </ul>	<p><i>Inter-Office Mail:</i></p> <ul style="list-style-type: none"> <li>• Mark outside envelope with “To be opened by addressee only”</li> <li>• Recipient to confirm receipt</li> </ul> <p><i>External Mail:</i></p> <ul style="list-style-type: none"> <li>• Use courier or registered mail</li> <li>• Mark outside envelope with “To be opened by addressee only”</li> </ul>
STORAGE	<ul style="list-style-type: none"> <li>• Commit password to memory</li> <li>• Reside in County approved business database or application</li> <li>• Keep hard copies and removable media (e.g. floppies, CD) in locked storage containers (e.g. in drawers or cabinets) when not in use</li> <li>• Store softcopies in home directory only.</li> <li>• Do not store on hard drive</li> <li>• Hard drives are prohibited from being removed from the device</li> </ul>	<ul style="list-style-type: none"> <li>• Keep hard copies and removable media (e.g. floppies, CD) in locked storage containers (e.g. in drawers or cabinets) when not in use</li> <li>• Reside in County approved business database or application</li> <li>• Store softcopies in home directory or in a restricted shared folder.</li> <li>• Do not store on hard drive</li> <li>• Hard drives are prohibited from being removed from the device.</li> </ul>	<ul style="list-style-type: none"> <li>• Keep hard copies and removable media (e.g. floppies, CD) out of sight (e.g. in drawers or cabinets) when not in use.</li> <li>• Reside in County approved business database or application</li> <li>• Store softcopies in home directory or limit access to shared folder.</li> <li>• Do not store on hard drive</li> <li>• Hard drives are prohibited from being removed from the device</li> </ul>
DESTRUCTION	<ul style="list-style-type: none"> <li>• Shred hard copies</li> <li>• Irretrievably erase (degauss) hard drives, disks, tapes or CDs (e.g. overwrite with a random pattern or physically destroy them)</li> <li>• Follow the Records</li> </ul>	<ul style="list-style-type: none"> <li>• Shred hard copies</li> <li>• Irretrievably erase (degauss) hard drives, disks, tapes or CDs (e.g. overwrite with a random pattern or physically destroy them)</li> <li>• Follow the Records Retention Schedule specific</li> </ul>	<ul style="list-style-type: none"> <li>• Shred hard copies</li> <li>• Irretrievably erase (degauss) hard drives, disks, tapes or CDs (e.g. overwrite with a random pattern or physically destroy them)</li> <li>• Follow the Records Retention Schedule specific to the type of record before destroying.</li> </ul>

**COUNTY OF SAN DIEGO  
ADMINISTRATIVE MANUAL**

SUBJECT: COUNTY DATA/INFORMATION – CLASSIFICATION,  
PROTECTION LEVEL, AND PROPER SECURITY

ITEM  
NUMBER **0040-09-02**

EFFECTIVE DATE: JUNE 5, 2008

PAGE 9 of 10

OPERATION	RESTRICTED	CONFIDENTIAL	SENSITIVE
	Retention Schedule specific to the type of record before destroying.	to the type of record before destroying.	
<b>LABELING AND MARKING</b>	RESTRICTED	CONFIDENTIAL	SENSITIVE

**I. Possible Consequences of Identified Misuses**

Observance of these policies and departmental procedures is essential to the delivery of County services and programs, and to the integrity, security and confidentiality of County data/information. Violation of these or other policies related to County data/information and information systems may constitute a failure to perform regular duties and assignments, and may result in any or all of the following:

- Reporting of the incident(s) to management;
- Possible revocation of access privileges;
- Possible disciplinary action, up to and including termination

**Approved:**



Walter F. Ekard  
Chief Administrative Officer

**Responsible Department(s):**

County Technology Office (CTO)  
Department of Purchasing and Contracting  
County Counsel

**CROSS-REFERENCES**

Board Policy A-54 (Public Access to County Records)  
Board Policy A-129 (Compliance with County-wide Records Management Program)  
Board Policy A-131 (Privacy Protection)  
Board Resolution 08-079 (Records Destruction)  
Administrative Manual section 0100-01 (Destruction of Records)

**COUNTY OF SAN DIEGO  
ADMINISTRATIVE MANUAL**

---

SUBJECT: COUNTY DATA/INFORMATION – CLASSIFICATION,  
PROTECTION LEVEL, AND PROPER SECURITY

ITEM  
NUMBER

**0040-09-02**

EFFECTIVE DATE: JUNE 5, 2008

PAGE

10 of 10

---

Administrative Manual section 0040-09 (Document and Records Management Program)  
Administrative Manual section 0040-09-01 (Emails; Verbal Communications; Voice Mail)  
Administrative Manual section 0040-09-03 (California Public Records Act procedures)

**Note: Additionally, one should check Departmental Records Retention Schedules and other Group, Department, Division or Office policies or procedures.**