MARICOPA COUNTY INTERNAL POLICY

Policy Title: **DATA CLASSIFICATION**	Policy Number:	A2244
	Current Adoption Date:	12-11-2024
	Current Implementation Date:	12-11-2024
Approved by: **BOARD OF SUPERVISORS**	Board Agenda Number:	C-41-25-005-X-00
	Original Adoption Date:	12-11-2024

I. PURPOSE

To ensure that Maricopa County and the Maricopa County Judicial Branch, collectively referred to as (County) protects the confidentiality, integrity, and availability of data generated, accessed, modified, transmitted, stored, or used by the County, irrespective of the medium on which the data resides and regardless of the format.

Users of County Technology Resources shall understand how data is classified so that proper security controls are applied to each data category based upon the identified security requirements and commensurate with the nature of the data in question. This policy requires the classification of data to ensure the required security measures are applied.

II. APPLICATION

This policy applies to all Maricopa County appointed departments, elected offices, the Flood Control District of Maricopa County, and the Maricopa County Library District (Special Districts). The Board of Supervisors is authorized to jointly adopt policies applying to the Special Districts under the Intergovernmental Agreement, C-06-18-393-6-00, approved on April 11, 2018.

The Judicial Branch (Superior Court, Adult Probation, Juvenile Probation, and Justice Courts) has agreed that the Judicial Branch will adhere to County information technology policies unless the Judicial Branch has an equivalent or more restrictive policy and provided County policies do not interfere or otherwise impede their ability to carry-out their required Constitutional and Statutory responsibilities nor restrict their ability to function as a separate and independent government entity.

III. DEFINITIONS

A. Appointing Authority: An elected official, the single administrative or executive head of a department/Special District, or the designated representative authorized to act in this capacity.

B. Chief Information Security Officer (CISO): The individual appointed by the County Chief Information Officer to hold responsibility over the security of the County's data and data systems.

C. County Chief Privacy Officer (CPO): An executive leadership role responsible for overseeing and implementing strategies to protect the County's information and to ensure compliance with HIPAA and other data privacy requirements.

D. County Data: Electronically Stored Information (ESI) owned by, contracted with, or controlled by the County; or used to conduct County business. The County may be a steward of the information; it does not need to originate within the County.

E. County Records Manager: An individual who has the statutory authority pursuant to A.R.S. § 41-151.14(A)(7) and responsibility to manage the records management program of the County and act as coordinator and liaison for the agency with the State of Arizona Library of Archives and Public Records.

F. County Technology Resource (CTR): Any computing account; device (e.g., mobile device, smartphone/tablet, computer, communications equipment, video conference, facsimile, or telephone); peripheral; software; local, wireless and wide area networks (i.e., LAN, Wi-Fi and WAN); Electronically Stored Information (ESI); website; cloud-based or internally-hosted system; or related consumable (e.g., disk space, processor time, network bandwidth) owned by, contracted with, or controlled by the County (Elected or Appointed Department) or by the Judicial Branch.

G. Data Classification Categories: The classification of County Data into one of three levels of sensitivity: Public Data, Restricted Data, or Confidential Data.

H. Data Owner: A position of executive leadership, normally the Appointing Authority, who, is accountable for data assets.

I. Data Steward: A position having functional authority and responsibility to manage and direct how County data is used within daily operations and routine business capacity. The Data Steward role is granted by the Data Owner and is usually a manager or supervisor of the Appointing Authority's office or department. The Data Steward assists the County Records Manager and County Data Privacy Officer in ensuring the department's compliance with this policy.

J. Department Records Coordinator (DRC): An individual who serves as the records coordinator for their department and assists the County Records Manager and County Chief Privacy Officer in ensuring the department's compliance with this policy.

K. Users: All workforce members (employees or any other individual performing work on behalf of, or with approval of the County) authorized to access CTRs. This includes County employees, temporary employees and non-employees providing products or services and/or who are given access to County Data such as suppliers on contract or outside organizations with IGAs.

IV. DELINEATION OF DATA, INFORMATION, AND RECORD

Data is information that can be used for reasoning, discussion, calculation, analysis, or decision-making.

Information is something that provides the answer to a question of some kind or resolves uncertainty.

A.R.S. § 41-151 provides the recognized definition of a record. The statute states, in part, that a record means all books, papers, maps, photographs or other documentary materials, made or received in pursuance of law or in connection with the transaction of public business and preserved or appropriate for preservation as evidence of the organization, functions, policies, decisions, procedures, operations or other activities or because of the informational and historical value of data contained in the record.

A record does not include library or museum materials made or acquired solely for reference or exhibition purposes, extra copies of documents preserved only for convenience of reference, and stocks of publications or documents intended for sale or distribution to interested persons.

Data and information can be held as a record. Data is the raw material, while records are structured and provide context to the data. Data and records may hold evidentiary or informational value within an organization's operations, governance and compliance frameworks, and are in most cases a public record.

V. POLICY

A. Data Classification

Data classification, in the context of information security, is categorizing data based on its level of sensitivity and the impact to the County should that data be disclosed, altered, or destroyed without

authorization. The classification of data helps determine appropriate security controls for safeguarding that data. Data Owners shall ensure that all County Data is classified according to one of the three Data Classification Categories: Public Data, Restricted Data, or Confidential Data. All data not specifically classified as Public Data or Confidential Data will be, by default, classified as Restricted Data.

1. Public Data

   Information that is available for general access without review by the Data Owner and/or County Counsel. Public Data, while subject to the Arizona Public Records Law, is available to all staff and to all individuals and entities external to the County. Data should be classified as Public when the unauthorized disclosure, alteration, or destruction of that data would result in little or no risk to the County. While little or no controls are required to protect the confidentiality of Public Data, some level of control is required to prevent unauthorized modification or destruction of Public Data.

2. Restricted Data

   Data categorized as Restricted requires security precautions to protect from its unauthorized use, access, or disclosure. Data should be classified as Restricted when the unauthorized disclosure, alteration, or destruction of that data could result in a moderate to high level of risk to the County. A reasonable level of security controls should be applied to Restricted Data (see Appendix A). By default, all County Data that is not explicitly classified as Confidential or Public should be treated as Restricted Data.

3. Confidential Data
   Confidential Data shall be protected from unauthorized use and/or disclosure by law, regulation, or standard, and requires the highest level of security measures (see Appendix A). Data should be classified as Confidential when the unauthorized use, disclosure, alteration, or destruction of that data could cause a significant level of risk to the County.

B. Required Security Controls

Note: All County Data (Public, Restricted, and Confidential) is subject to the retention schedules set by the State under A.R.S. §§ 41-151.12(A), 41-151.15, and 41-151.19.

1. Public Data

   Public Data requires only limited access restrictions and may be made available for public access. Public data can be stored and transmitted without restriction. Documented backup and recovery procedures are not required, but strongly encouraged for business continuity.

2. Restricted Data

   Restricted Data may be accessed by users who have a business “need to know” as determined by the Data Owner or Data Steward. Restricted Data can only be transmitted through systems authorized for such use by the CISO or authorized designee. The security controls used to protect stored Restricted Data is at the discretion of the Data Owner in accordance with standards set by the CISO. Backup and recovery procedures for Restricted Data and associated data systems shall be documented.

3. Confidential Data

Confidential Data may be accessed by users who have a business "need to know" as determined by the Data Owner or Data Steward. Access, use, storage, or transmission of Confidential Data by third parties shall be governed by contract, non-disclosure agreement (NDA), or business associate agreement(s) (BAA). Transmission of Confidential Data shall be encrypted in accordance with standards set by the CISO. Storage of Confidential Data is in accordance with standards set by the CISO and prohibited on unauthorized CTR unless otherwise approved by the CISO. Backup and recovery procedures for Confidential Data and associated data systems shall be documented.

C. Monitoring Controls

1. Data Owners with responsibility for Confidential Data shall ensure security controls are in place that segregate, encrypt, and protect Confidential Data in accordance with standards set by the CISO. These controls shall be actively monitored and conform to incident response and breach reporting procedures for potential misuse and/or unauthorized access. Within Enterprise Technology & Innovation (ETI) supported departments, these monitors are established; equivalent or better monitoring solutions shall be established in non-ETI-supported departments. Data Owners are also required to submit an annual report to the CISO outlining departmental security practices and training participation.

2. Data Owners with responsibility for Restricted Data shall collaborate with IT provider to monitor and review their systems and procedures for potential misuse and/or unauthorized access at minimum quarterly or more frequently as deemed necessary by the Data Owner or CISO. Within ETI-supported departments, these monitors are established; equivalent or better monitoring solutions shall be established in non-ETI-supported departments.

3. No monitoring controls are required for Public Data. However, retention schedules still apply to Public Data that fits the definition of a public record.

D. Loss or Unauthorized Disclosure of Confidential Data

1. The CPO shall be notified at the time of discovery if data classified as Confidential is lost and/or destroyed, disclosed to/accessed by unauthorized parties, or suspected of being lost and/or destroyed, or disclosed to/accessed by unauthorized parties.

2. In the event of compromised or breached Confidential Data, notification shall be conducted pursuant to County Policy A2237 Reporting of Security Events, Security Incidents, and Breaches and/or other relevant statutory data regulations.

VI. AUTHORITY AND RESPONSIBILITIES

A. Chief Information Security Officer (CISO)

The CISO will apply necessary priority and resources to implement a Data Classification program by:

1. establishing an Information Security program to issue guidance for data classification and to receive data incident reports, analyze those reports, and take appropriate incident response actions for data incidents.

2. providing the ETI-supported network enterprise community with information systems that have been configured with proper technical controls to organize data into each of the Data Classification Categories.

3. collaborating with non-ETI-supported departments to ensure systems County-wide have similar technical controls.

4. establishing a communications plan that incorporates bi-directional flow of information between ETI and Data Owners or designees throughout the County and Judicial Branch.

5. establishing a minimum standard of security controls for each Data Classification Category, using guidance from the National Institute of Standards and Technology (NIST) Cybersecurity Framework and HIPAA HITECH to apply data security, including for services related to encrypted electronic transmissions.

6. establishing user-awareness training guidance to assist departments in applying Data Classification Categories to County Data.

7. establishing guidance for system and application developers who shall apply security controls to protect County Data at all levels of data classification.

8. maintaining this policy by reviewing and updating annually.

9. implementing a Data Loss Prevention (DLP) initiative that tags information system resources used to process Confidential and/or Restricted Data resources.

B. County Chief Privacy Officer (CPO)

The CPO will apply necessary priority and resources to support a Data Classification program including:

1. Collaborate with the County Records Manager to:

   a. establish departmental guidelines for Users on practices and procedures to implement Data Classification programs to help identify Confidential Data and properly validated public records, or records that are open to the public.

   b. develop policy to guide Users on practices and procedures for granting and terminating access to, or disposition of, Confidential and Restricted Data.

   c. develop policy to guide Users on practices and procedures for vetting County data for public release.

2. Ensure all reports of known or suspected breaches of Confidential data are investigated and reported in accordance with current relevant data regulation requirements.

C. Data Owners

Data Owners will apply necessary priority and resources to support a Data Classification program including:

1. In accordance with County Policy *A2611 Use of County Technology Resources*, ensure appropriate CTR monitoring, and report security events as specified.

2. Work with the Information Governance Department to incorporate appropriate methods and business practices to validate, authorize, and categorize Public Data prior to public release.

3. Ensure the monitoring of security controls that are established to protect Confidential and Restricted Data.

4. Ensure security controls required to protect data classified as Confidential or Restricted are established and monitored.

5. Coordinate with the CISO and CPO to ensure the system and data controls in use comply with current applicable data regulations and standards.

6. Data Owners with responsibility for Restricted and/or Confidential Data must monitor and review their systems and procedures for potential misuse and/or unauthorized access at minimum quarterly or more frequently as deemed necessary by the Data Owner or CISO.

7. Ensure appropriate classification of data and implementation of applicable security requirements per classification category.

8. Ensure that users receive the appropriate training, and that they review and acknowledge this policy annually.

9. Identify a subject matter expert within their department to provide guidance and management decisions on how data will be classified, controlled, and shared.

10. Implement standard practices to identify and properly file County data by its appropriate Data Classification Category.

11. Ensure that security incidents of unauthorized access, use, or disclosure of Confidential Data are promptly reported to the County CPO.

12. Oversee the classification of County Data per the Data Classification Categories established by this policy and coordinate with the CISO on implementation of security measures/requirements/controls as applicable for each category of data.

13. Assign at least one senior level employee to serve in the role of Data Steward. Classification of data should be performed by an appropriate Data Steward.

14. Within one (1) business day of a change, notify the CISO and CPO when an individual serving as Data Owner or Data Steward is added or removed from their role.

15. Ensure that the employee designated as the DRC, per County Policy A2101 Records Management, coordinates with the Data Steward and applies appropriate security policy, practices, and protocols associated with the Data Classification Category of each record under this policy.

16. Incorporate daily operations that include default Restricted Data classification applied to County data resources until a data review results in a classification of Public Data or Confidential Data.

17. Organize data in such a way as to be prepared, at any time, to respond to legally required electronic discovery, record requests/subpoenas, preservation holds, inspections, or other access and make changes in Data Classification Category as appropriate. These may be initiated by legal counsel, court order, public records request, or governing policy or law and may require the means to quickly identify and control data resources for data classification.

D. Users

Individual Users of County Technology Resources will:

1. apply data classification practices to achieve data protection in compliance with County Policy *A2611 Use of County Technology Resources*, and other relevant security policies that direct user responsibilities for protecting County data resources.

2. be aware of and employ the security standards of this policy and identify their responsibilities for each category of data: Public, Restricted, and Confidential.

3. immediately report any known or suspected data security incidents (e.g., destruction of data outside of established policy and procedure, virus/worm attacks, actual or suspected loss or unauthorized disclosure of Confidential Data) or system vulnerability to the County Information Security Team in accordance with County Policy *A2611 Use of County Technology Resources*.

E. Human Resources (HR):

1. Ensures this policy is included in the New Employee Orientation (NEO).

2. Ensures policy updates are distributed electronically to all employees.

3. Supports the Data Owner in the tracking of annual employee acknowledgment of this policy.

VII. COMPLIANCE

Violation of this policy may result in disciplinary action up to and including termination. All reported violators, including non-employees, shall be referred to appropriate department executives. In addition to internal disciplinary measures, individuals found in violation of this policy may be subject to criminal prosecution, civil liability, or both. Exceptions to this are at the discretion of Appointing Authorities and their designees as deemed appropriate in activities related to legitimate use.

The CISO, or designee, is authorized to initiate investigations of violations of this policy and other information technology security standards.

The Maricopa County Internal Audit Department may conduct periodic audits to evaluate and ensure compliance with this policy. In some circumstances, outside technology and security auditors may perform audits of CTR and information technology operations.

Revision History

Version	Revision Date	Description of Revision
1	12-11-2024	Initial version. (C-41-25-005-X-00)

APPENDIX A: Maricopa County Data Classification Table

	Confidential (highest, most sensitive)	Restricted (moderate level of sensitivity)	Public (low level of sensitivity)
Reputation Risk	High	Medium	Low
Description	• Data which is legally regulated • Data that would provide access to confidential or restricted information	• Data which the Data Managers have decided not to publish or make public • Data protected by contractual obligations	• Data for which there is no expectation of privacy or confidentiality
Legal Requirements	• Protection of data is required by law	• Protection of data is governed by contractual terms or is otherwise at the discretion of the Data Owner or Data Steward	• Protection of data is at the discretion of the Data Owner or Data Steward
Data Access and Control	• Legal, ethical, or other constraints prevent access without specific authorization • Data is accessible only to those individuals permitted under law, regulation, or County policy, and with authorized access • Authorization typically depends on the applicable law and a business "need to know"	• May be accessed by County employees • May be accessed by non-employees who have a business "need to know"	• Limited access restrictions • Data is available for public access
Transmission	• Unencrypted transmission of Confidential Data through any non-County network or County guest network is prohibited (e.g., Internet) • Unencrypted transmission through any electronic messaging system (e-mail, instant messaging, text messaging) is prohibited • Confidential Data may be redacted/deidentified instead of encrypted	• Unencrypted transmission of Restricted Data through any wireless network, and any non-County wired network is strongly discouraged. Where necessary, use of County VPN is required • Unencrypted transmission through any electronic messaging system (e-mail, instant messaging, text messaging), is at the discretion of the Data Owner or Data Steward	• No protection is required for public information; however, care should always be taken to use all information appropriately • Applicable retention schedules and the Public Records Request policy must be followed

*table continued on next page

Storage	• Storage of Confidential Data is prohibited on unauthorized County Technology Resources or a personal device unless approved by the Chief Privacy Officer • If approved, ETI approved encryption is required on mobile Computing Equipment • ETI approved security measures are also required if the data is not stored on a County Technology Resource • Storage of credit card data on any County Technology Resource is prohibited	• Level of required protection of Restricted Data is at the discretion of the Data Owner or Data Steward of the information • If appropriate level of protection is not known, check with Chief Privacy Officer before storing Restricted Data unencrypted	• No protection is required for public information; however, care should always be taken to use all information appropriately • Applicable retention schedules and the Public Records Request policy must be followed
Applicable Documented Backup & Recovery Procedures	• Documented backup and recovery procedures are required	• Documented backup and recovery procedures are required	• Documented backup and recovery procedures are not required, but strongly encouraged
Documented Data Retention Policy	• Documented data retention policy is required	• Documented data retention policy is required	• Documented data retention policy is not required, but strongly encouraged
Monitoring Controls	• Data Owners and Data Stewards with responsibility for Confidential Data shall actively monitor and review their systems and procedures for potential misuse and/or unauthorized access	• Data Owners and Data Stewards with responsibility for Restricted Data shall periodically monitor and review their systems and procedures for potential misuse and/or unauthorized access	• No monitoring controls are required

APPENDIX B: Data Examples (not all-inclusive)

***Exceptions apply**

Confidential (highest, most sensitive)	Restricted (moderate level of sensitivity)	Public (low level of sensitivity)
Personally Identifiable Information (PII) Regulated by Federal, State (e.g., A.R.S. § 18-552), or Local law* Last name, first name or initial with any one of following: • Social Security Number (SSN) • Driver's license • State ID card • Passport number • Taxpayer ID number or identity protection personal ID number issued by the IRS • Health insurance ID number • The individual's medical or mental health treatment or diagnosis by a health care professional • Biometric data • Financial account number or credit card or debit card number in combination with any required security code, access code/pin, or password that would allow access to the individual's financial account **continued on next page*	**Personal/Employee Data** • Employee ID number • Income information and payroll information * • Personnel records, performance reviews • Race, ethnicity, nationality, gender • Date and place of birth • Directory/contact information designated by the owner as private • Employment data, claims, and information that is not classified as Confidential Data **Business/Financial/Departmental Data** Financial transactions that do not include: • Confidential Data • Information covered by non-disclosure agreements • Credit reports • Records on spending, borrowing, net worth • County vendor or partner information where no restrictive confidentiality agreement exists • Personally identifiable information collected from the public in order for the County to provide services to those individuals, that is not classified as Confidential Data **continued on next page*	**County Information Designated Public** • Board agendas and meeting minutes • Budgets • Policies • Approved contracts, IGAs, and MOUs • Published press releases • Department information and services, as published on County websites • Published newsletters, ordinances, meeting information, and County maps • Job descriptions, job postings, market range titles/salaries • Marketing materials intended for the general public • Unpublished data that could be made public

Protected Health Information (PHI) Regulated by HIPAA* • Health status • Healthcare treatment • Healthcare payment **Substance Use Disorder Records Regulated by 42 C.F.R. Part 2*** **Criminal Justice Information (CJI) Regulated by Federal, State, or Local Law*** • Law Enforcement sensitive information **Online Account Information*** • Individual's username or e-mail address, in combination with a password or security question and answer, that allows access to an online account **Business/Financial Data Regulated by Federal, State, or Local Law** • Credit card numbers with/without expiration dates	**Systems/Log Data** • Server event logs	