Internal Use Only
UNADOPTED DRAFT

Williamson County Information Technology

Data Management Policy

Sensitivity: None
Criticality: High
Primary Type: Policy

Summary

Purpose

This policy establishes the parameters for *classification* and *management* of electronic data and paper records. This document acknowledges and is supplemented by the Records Management Plan for Non-Elected Williamson County Offices and Archives Records Storage Center, now known as the Non-Digital Records Management Plan for Non-Elected Offices.

The primary objectives for *data classification* are to (A) protect data integrity, (B) preserve data confidentiality, and (C) ensure availability of data to those permitted to access and utilize the data in the performance of assigned or assumed duties.

Data classification parameters shall be based on pertinent state and federal statutes and regulations, county policy, and currently accepted approaches appropriate for the (global) geopolitical and cybersecurity environment. These classifications shall be used to define control objectives for collection, transmission, use, storage, and distribution of data by the County in conducting business and shall aid in assignment of priority given during support, maintenance, and disaster recovery.

Two criteria used in data classification are *confidentiality* and *criticality*. Williamson County shall employ safeguards to protect against unintended changes in data or disclosure of confidential, sensitive, and/or critical data. In accordance with the intended spirit of state and federal law, Williamson County will remain transparent with public data.

Scope

This policy is platform and technology neutral and applies to all electronic data and information used by Williamson County for conducting county business. It applies to all users as defined in this document below. Retention of hardcopy physical records is not absolutely within the scope of this document. ***For physical record retention and procedures, reference should be made to the Non-Digital Records Management Plan for Non-Elected Offices.***

Definitions

Confidentiality
A measure of how protected data must be against unwarranted disclosure or modification. Data is considered confidential if its disclosure results in, or could reasonably result in, a violation of law or court order, or could reasonably constitute criminal activity.

Criticality
A measure of the importance of an information system, or its information to serve a public or departmental function.

Data
Discrete raw bits of fact that, when collected, analyzed, and interpreted establish information.

Data Custodian
The user(s) responsible for *storage and safeguard* of computerized data.

Data Owner
The user(s), normally a manager or director, who has responsibility for the integrity, accurate reporting, and use of computerized data.

Data Transmission
Transfer of data by any means (physical or electronic) from any repository to another.

Department
Unless specifically noted otherwise, the use of the word "department" or related forms includes both Commissioners Court departments and all elected offices that utilize the Williamson County technology infrastructure.

FIPS-199
FIPS 199 (*Standards for Security Categorization for Federal Information and Information Systems*) is a publication issued by the National Institute of Standards and Technology within the U.S. Department of Commerce. It provides a standardized way to categorize information and information systems in a secure way.

Government Record
A record that is created, collected, stored for, or used by the government for transaction of business by an employee, officer, elected official, or agent of the government.

Information
Collection(s) of **data** which have been processed, interpreted, organized, and structured.

Information System
Any technology used to collect, process, store, transmit, or display data in support of county department business objectives

Protected Data or Information
Data or collections of data which are subject to access control as *legally* required for the protection of an individual's identity, health, safety, privacy, or reputation; and for the protection of the integrity of data used by the county to accomplish the county's objectives.

Record
A collection of meaningful data and information assembled into a document, paper, report, letter, book, map, photograph, sound, or video recording, regardless of its classification.

Redaction
The masking or removal of Confidential or Protected Data or Information prior to authorized release.

Risk

The combination of the probability of an adverse event and its potential impact; relative measure of the absence of absolute safety and security.

Security Controls
Physical, technical, and administrative controls put in place to ensure successfully maintained confidentiality, integrity, and availability of data as well as the systems used to manage, access, and use that data.

Sensitivity
A measure of how much harm could occur were data or information to be disclosed without due process and consideration. Sensitive information is more closely associated with personal identity. Data is considered sensitive if its disclosure could reasonably result in harm or undue hardship to (an) individual(s).

TSLAC
Texas State Library and Archives Commission

User
Any employee, elected official, volunteer, intern, external agency employee, vendor, contractor, or 3rd-party that accesses Williamson County information, information system(s) or devices(s).

Policy

Data shall be collected, stored, protected, accessed, released, and destroyed by Williamson County according to the data's intended purposes, classifications, and retention requirements or as otherwise required by law. Any standards, procedures and guidelines created by county offices and departments pertaining to management of electronic data shall be subject to this policy.

A. Data Management Principles

1. Management of Williamson County's Government Records shall:
    a. Be based on the value and risks associated with the data;
    b. Meet or exceed appropriate levels of protection as required by law;
    c. Account for ethical, legal, proprietary, and privacy considerations; and
    d. Recognize that data classifications are contextual and subject to change. Assigned Data Classifications shall be periodically reviewed.
2. Ownership and Availability of County Data
    a. Regardless of form or format, all data which is used, gathered, or created at the cost of Williamson County or in support of the transaction of County business shall remain the property of the County.
    b. Data Owners shall be responsible for appropriate classifications of data's confidentiality and criticality.
    c. Data Custodians shall be responsible for the appropriate safeguard of data based on its classification.
3. Retention of data shall be:
    a. in accordance with pertinent TSLAC Retention Schedules and any applicable state and federal statutes and regulations; and

b. in a manner allowing it to be reliably accessible to intended audiences, and in accordance with relevant County Data Loss Prevention Standards and Procedures.

B. Data Classifications

1. **Confidentiality / Sensitivity**
   Confidentiality is determined by the Data Owner and based on federal and state law and regulations, standards, and/or industry best practices applicable to local governments and specific business segments. Questions regarding classification of data shall be addressed by Data Owners with guidance of Williamson County's General Counsel.

   a. **Low (None):**
      1. Neither confidential nor controlled in its distribution.
      2. Integrity and accuracy of data and information shall be maintained by custodian.
      3. In accordance with the intentions of the Texas Public Information Act, this data and information ***may*** be posted in common areas accessible by all users.
      4. Examples: Statistical reports, quick fact sheets, unrestricted directory information, general educational content available to the public at no cost, social media posts by Public Information Office, government meeting notes and agendas required to be publicly posted by law.

   b. **Moderate (Controlled)**:
      1. Intended for limited distribution.
      2. May present the risk of security compromise or other (financial / asset) loss if disclosed to unauthorized or malicious groups or individuals.
      3. Public release may be subject to redaction of sensitive elements.
      4. Consultation with document author(s) is recommended prior to release of information to the public domain.
      5. Examples: Security-related information

   c. **High (Confidential / Restricted)**:
      1. Data and information are specifically protected by state and/or federal law (e.g., HIPAA, CJIS, FERPA, PCII) or deemed protected by a recognized court.
      2. Unwarranted disclosure would be a violation of federal or state regulations, contractual constraints and/or legally binding order.
      3. Examples: Patient information, protected health information (HIPAA), certain student education records (FERPA), credit card numbers (PCII), social security numbers, criminal justice information (CJIS).

2. **Criticality**
   Criticality is defined with guidance prescribed by **FIPS-199**. Data Owners are responsible for establishing criticality classifications. Data Custodians are responsible for application of security controls for protection of data confidentiality, integrity, and availability.

   a. Low
   Loss of confidentiality, integrity, or availability could be expected to have a **limited** adverse effect on organizational operations or assets. Adverse effects on individuals

may include but are not limited to, loss of the privacy to which individuals are entitled to under law.

LIMITED adverse effect examples:

- Cause a degradation in mission capability to an extent and duration that the organization can perform primary functions, but *effectiveness and efficiency are noticeably reduced*.
- Result in *minor damage* to organizational assets.
- Result in *minor financial loss.*
- Result in *minor harm* to individuals.

b. Moderate

Loss of confidentiality, integrity, or availability could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.

SERIOUS adverse effect examples:

- Cause a significant degradation in the mission capability to an extent and duration that the organization can perform its primary function, but the effectiveness and efficiency is significantly reduced
- Result in significant damage to organizational assets
- Result in significant financial loss
- Result in significant harm to individuals that does not involve loss of life or serious life-threatening injury

c. High

Loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

SEVERE or **CATASTROPHIC** adverse effect examples:

- Cause severe degradation in or loss of mission capability to an extent and duration that the organization is *not able to perform one or more* of its primary functions
- Result in major damage to organizational assets
- Result in material financial loss
- Result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries

C. Data Storage and Protection

1. Users with access to county data shall attest to receipt of this policy, and comply with other county policies governing access to information and information systems, specifically including:
    a. Acceptable Use Policy and associated documents
    b. Access Controls Standard and Procedures and associated documents
    c. Cybersecurity Awareness Training Policy
    d. Pertinent departmental standards and procedures for information management

2. Regardless of data classification or form, all data useful to the County and its constituents shall be protected against accidental or malicious disclosure, modification, ransom, or destruction.
    a. Data protection methods (e.g., backup or redundancy), shall be adequate to meet business continuity and disaster recovery requirements for each dataset.

b. Where a Williamson County IT user serves as Data Custodian, Data Owners shall define protection requirements for each data set in coordination with IT staff.

3. Backup data shall have at least the same levels of protection as required for the original source data. Retention of backup data shall allow for adequate business continuity and disaster recovery objectives.
   Specific protection applied to data shall:
   a. Have availability based on classifications defined in this document; and
   b. Apply to protection of data and information:
      i. During data transmission or storage; and
      ii. Against unintended and unwarranted modification or distribution until the end of its retention period or until its destruction.

4. To ensure adequate and appropriate protections can be applied to electronic data, only county-provided tools, applications, machines, and services shall be used for data collection, sharing, and storage. Non-County managed tools are expressly prohibited for the creation or storage of **Protected Data or Information** as defined herein. ***Confidential data shall not be transmitted using personal, non-county-managed cellular devices***.

5. ***Use of unapproved information storage, exchange, or collection services (including but not limited to Dropbox, Google, Yahoo, unencrypted removable USB or disk drives, and other similar services) for primary or copied instances of ANY county-owned protected data is expressly prohibited.*** Such sites and services may not afford the levels of protection appropriate to guard against data compromise or data loss.

6. Vendors and agents of Williamson County shall adhere to applicable principles established by this policy and adherence shall be accounted for in Business Associate Agreements (BAA) and other contractual acknowledgements. Data Owners are responsible for the accounting of those BAA and signed agreements.

D. Records and Information Release

1. Any records as defined in this policy shall only be released to recipients through established due process using established channels for records requests. Records requests shall be directed to:
   a. Williamson County Attorney's office for non-law enforcement related records
   b. Williamson County HR for employee-related records
   c. For law enforcement related records, the office of the elected official with jurisdiction
   d. The office and data owner with charter to routinely release records and information for business purposes, with guidance from Williamson County Legal Counsel or the County Attorney's office.
   e. The Public Affairs office should be consulted for release of information associated with potential media interest.
2. Certain data may be considered explicitly protected for interests of County or personnel security

E. Examples of Explicitly Protected Data

Examples of data and information that are explicitly protected and should be treated with the highest protection available include, but are not necessarily limited to:

1. Login Credentials for information systems
2. Information protected by regulatory agencies (FERPA, CJIS, HIPAA, etc.)
3. Credit card details
    a. 16-digit numbers
    b. Expiration dates
    c. CVV number
4. Sensitive financial details (user or non-user)
5. Sensitive personal information (user or non-user)
6. Non-public information related to competitive bidding (RFPs, trade secrets, etc.…)
7. Information protected by privilege (doctor-patient, attorney-client, etc.…)
8. Information exempted from disclosure under state open records laws
9. Information or facts related to critical infrastructure security or critical business functions which could reasonably pose threat of loss to the public interest if disclosed

F. Specific Protection Required

Some data are subject to special consideration and prohibited from disclosure under federal and / or state laws and judicial rules. These data shall be classified and managed accordingly by Williamson County Data Owners and Data Custodians.

Exceptions

Compensating security controls may be required for exceptions to this policy.

Exceptions to technology-related policies, standards, and procedures **may be** conditionally granted, and **must be** documented via the Policy Exception Procedure and approved by the department head of the department requesting the exception, and by Williamson County ITS.

Certain exceptions may require authorization by or consultation with Williamson County Human Resources, Purchasing, Facilities, Legal Counsel, Risk Management, Auditor's Office, Budget Office, and/or Commissioner's Court.

Conflicts

Any ambiguities, conflicts, or questions related to this policy in conjunction with any other policy or legal authority should be referred to the Chief Information Officer for Williamson County ITS.

Violations

Violations of this policy or suspected security breaches shall be immediately reported to Williamson County Information Technology and remediated within a period determined to be reasonable by the Data Owner and Data Custodian for the data or information systems not in compliance with this policy.

Violations of this policy are subject to immediate remediation in the interest of the security of county assets and resources. Immediate remediation may involve quarantine of hardware from connection to Williamson County Information Systems.

Violations of this policy may constitute concurrent violation of the Williamson County Acceptable Use Policy, and result in escalating disciplinary actions up to and including termination of employment.

Misuse or abuse, intentional or unintentional, malicious, or benign, of electronic systems and services may result in immediate, temporary suspension or permanent revocation of user credentials and disciplinary action, up to and including termination of employment.

Related Statutes, Policies, and Authorities

County

Acceptable Use Policy
Access Control Policy
Access Controls Standard and Procedures
Cybersecurity Awareness Training Policy
Cybersecurity Guidelines for Users Processing Public Email
Data Loss Prevention Standard and Procedures
Non-Digital Records Management Plan for Non-Elected Offices

State

Texas Local Government Records Act (Title 6, subtitle C, Texas Local Government Code)
Texas Public Information Act (Chapter 552, Texas Government Code)
TSLAC Local Government Retention Schedules, current amendment

Federal

FEDERAL INFORMATION PROCESSING STANDARDS (FIPS) 199: *Standards for Security Categorization of Federal Information and Information Systems*

Contact Office

Except as otherwise stated herein, the contact for questions or clarifications pertaining to this policy may be directed to a user's department leadership. Department leadership should contact the ITS Service Desk for appropriate routing. ITS Service Desk hours are 0500 – 2000 on county working days.

Employee Portal: ServiceNow
Email: servicedesk@wilco.org
Phone: 512-943-1456

Administrative Notes

Policy Class: Risk Management
Policy Family: Information Security
Policy: Data Management Policy

Responsible: ITS Director of Policy
Accountable: ITS CIO
Consulted: Human Resources, Risk Management, Legal Counsel
Informed: All Users with Attestation

Revision History

Version	Date	Description
2.0		Adoption by Williamson County Commissioners Court
1.1	11/22/2022	Incorporate changes based on HR, Legal, Risk Management feedback.
1.0	9/22/2022	First version towards ITS GRC Engineering, CIS, NIST compliance.