Williamson County Information Technology

Access Control Policy

Sensitivity: None
Criticality: High
Primary Type: Policy

Summary

Purpose
The purpose of this policy is to establish access controls to be applied to information systems in the interest of

A. Protecting data, information, and information systems integrity
B. Preserving restricted access to sensitive and confidential information, and
C. Ensuring availability of information and information systems to those permitted to access and use them in performance of assigned or assumed duties

The primary objective for implementing access controls is to ensure that users accessing information systems are doing so within the scope and authority of their functions. This is a necessary safeguard against unintended or unwarranted modification of data and information contained within those systems. It is also a safeguard against unauthorized disclosure of information protected by law. This policy provides guidance for the management and use of access controls regulating access to Williamson County information systems.

Scope
This policy is platform and technology neutral and applies to all information systems used by Williamson County for conducting county business. It applies to all users as defined in this document below.

Disambiguation: Except for below headings addressing physical access to server rooms, this policy does not apply to physical or perimeter access to county-managed facilities. Physical access policy direction and documentation shall be provided and managed by Williamson County Facilities.

Definitions

Access Controls
The processes, rules and deployment mechanisms that control access to information systems, resources, and physical access to premises

Administrative Controls
Documented and adopted policy, standards, procedure, processes put in place to help uniformly regulate operations and controls that are not implemented by technology

Application Owner
Employee(s) that have been designated the primary manager(s) of an information system

Asset and Service Management System / ITIL System
ServiceNow

Authentication
The act of verifying the identity of a user and/or the user's eligibility to access information systems

Business Associate
A non-county-employed individual or organization performing functions, activities, or services on behalf of Williamson County

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

Department Head
A user or employee responsible for fiscal activities under the budget cost center(s) for which they have signature approval authority (or) the chief official responsible for the activities within the domain of their primary jurisdiction and charter

Department Liaison to ITS
A non-ITS user or employee who is not a department head, but is delegated the authority to make decisions regarding identity assignment, system configuration, or administration of non-ITS-managed information systems

Employee Asset / Hiring Manager
A department level employee responsible for ServiceNow asset management requests, asset assignments, and termination of asset access.

ITS-Managed Information System
An information system that is managed or administered by Williamson County ITS (e.g., Kronos, Telestaff, Oracle, Microsoft 365, Agenda Quick, Performance Center).

Identifier/Identity
A unique username or other mechanism assigned to an individual person for use in gaining user-level access to information systems or information

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

Least Privilege
A risk management concept wherein only the least amount of access needed to accomplish a business objective is enabled by default or subsequent authorization. The practice of least privilege is incorporated to ensure certain information or system functionality is not exposed to risk of compromise or misuse

Mobile Device
Any portable information system used in support of county business objectives. Examples include, but are not limited to, smart phones and tablets, but **do *not*** include laptop computers

Multi-Factor Authentication
A combination of more than one authentication method, such as token and password (or personal identification number [PIN] or token and biometric device)

Non- ITS Managed Information System
An information system that is NOT managed or administered by Williamson County ITS

Password
A protected, generally computer-encrypted string of characters that authenticate a computer user for access to a computer or information system

Peripheral Hardware Device
An auxiliary device that connects to and works with a computer to (A) put information into it or (B) get information out of it for purposes of enhancement of desired function or result. May include data storage device (USB), audio, video, networking, or communications device connected to a computer wirelessly or by physical connection

Privileged Account
A user account that enables an individual to establish or modify identification or authority credentials, access rules, production applications, application feature sets, operating system functions or network parameters and rules

Restricted/Confidential Information
Information or data classified as **Confidential** by Williamson County Data Management Policy

Service Account
A user account that is created explicitly to run a particular function or service on an operating system for an application

Service Management System / ITIL System
ServiceNow

Single Sign On (SSO)
An authentication scheme that allows a user to log in with a single ID and password to any of several related, yet independent, information systems. True single sign-on allows the user to log in once and access services without re-entering authentication factors

System Administrator
A user(s) who manage(s) the operation of an information system or particular electronic communication service

Technical Controls
The policies, procedures, organizational structure, and electronic access controls put in place to help ensure security (confidentiality, integrity, and availability) of information systems

Technology Asset
Any technology device or software/software license/software subscription used in the performance of assigned duties or connected to any network paid for by Williamson County or maintained by Williamson County Information Technology Services (ITS)

Termination Request
A request to cancel all user access to information systems due to departure of the individual from Williamson County

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)

User-Level Access
Any attempt to access an information system or obtain information initiated by an individual person

Roles and Responsibilities

- Users are required to adhere to this policy while using any county information system.
- Elected Officials and Department Heads are required to ensure all employees are informed of this policy and that each employee fully understands and undertakes to comply with this policy.

Policy

For both ITS-managed and non-ITS-managed information systems, administrative and technical controls shall be adopted to ensure the security of information systems in the interest of preserving the integrity, confidentiality, and availability of the data within those systems. This policy and supporting standards and procedures define minimally necessary parameters for managing access control.

Supporting department level standards and procedures may build upon these minimum parameters but must not conflict with this policy and associated standards.

A. Access Control

1. General Principles
    a. User Identity
        i. All users shall be assigned a unique username (identity) by Williamson County ITS.
        ii. A unique email address shall be associated with each user identity assigned to employees by Williamson County ITS on or shortly after their date of hire and communicated to the employee via Williamson County Human Resources.
        iii. The identity assigned by ITS shall be the representation of a user for purposes of regulating access and permissions as well as for tracking cyberactivity.
    b. User Password(s)
        i. Temporary passwords shall be changed after one use.
        ii. Passwords shall be managed in accordance with Williamson County Access Controls Standard and Procedures
        iii. Passwords for **any** information systems shall be reset if there is reason to believe that a user's account has been compromised.
    c. Least Privilege and Role Based Access, Temporary Elevation of Privilege
        i. Employees shall be granted the lowest level of permissions necessary to accomplish assigned duties efficiently
        ii. Temporary elevation of privilege may be extended for higher-level administrative or temporary duty assignments

iii. Such temporary changes in permission shall define an explicit and reasonable time constraint, and shall be documented:
   1. By electronic logging within the information system(s) or
   2. Within the ITS Service Management System (i.e., as an asset assigned to the employee by the Employee Asset / Hiring Manager)

2. Hardware Access to Information Systems
   a. **ALL hardware devices not obtained from ITS, including hardware drivers,** connected to Williamson County information systems shall be authorized formally by ITS in writing.
   b. Hardware that is capable of being monitored for security purposes shall be monitored by security monitoring information systems deployed by ITS.
   c. TRUST CERTIFICATES: Computers normally able to access the Williamson County network **shall be isolated from access to the network** if not logged in to the network for a time period defined in Access Controls Standard and Procedures. Following the defined period of inactivity, users of these devices shall not be able to use the devices without ITS intervention.
   d. Hardware that is discovered to be deployed without the documentation required by this policy shall
      i. If there is apparent threat to the cyber environment: be subject to being disabled by ITS and quarantined until the hardware can be deemed secure for use within the Williamson County environment.

         Affected department head(s), elected official(s), and/or department liaisons to ITS shall be immediately notified by a member of ITS management of any unauthorized device upon disabling and quarantine.

         OR

      ii. If there is no apparent threat to the cyber environment: ITS shall notify the affected department prior to disabling. The department may request an exception for continued use while the device is assessed for security approval.
   e. Security assessments shall be conducted and dispositioned in cooperation among departments and ITS.
3. Physical Access to Server Rooms and Data Centers
   a. **Physical access to rooms containing servers shall be restricted to authorized personnel**.
   b. No equipment other than approved equipment or devices shall be introduced to, removed from, or modified within the Williamson County network environment, including server racks or connections within server rooms, without consent in writing from Williamson County ITS.
4. Shared Devices Caution
   a. ***Shared devices may incorporate the use of Single Sign On (SSO)*** for employee access to certain Information Systems (e.g., Office 365, Oracle). To avoid inadvertent unauthorized access using identities of others, users shall ensure that they are authorized to use the account to which they have access.

5. Management and Inventory of User Access
    a. Granting and Revocation of Access to Information Systems shall be in accordance with the Williamson County Access Controls Standard and Procedures.
    b. Permission to access ITS-managed information systems shall be recorded in the employee's list of assigned assets in the Asset and Service Management System / ITIL System

6. Foreign Travel Notification shall be made for users working or accessing work-related content from locations outside of the United States.

B. Authorized Identity

1. Individual User Accounts
    a. Shall be used for specific information system access and record creation or modification
    b. The use of technology access controls shall be applied where possible (e.g., session idle timers, IP access restrictions, password complexity rules, multi-factor authentication, Single Sign On)

2. Multiple Factor Authentication (MFA)
    a. Only approved methods of MFA will be accepted as defined in the Access Control Standards and Procedures.
    b. User accounts with access to information systems containing **Confidential** data as defined in the Williamson County Data Management Policy from outside of the county-managed network shall be subject to ITS-approved multiple-factor authentication and comply with the Access Controls Standard and Procedures, and current CJIS Policy.

3. Generic User Accounts
    a. Are strongly discouraged, AND
    b. Shall be **inventoried and maintained** by ITS within Active Directory, AND
    c. Be assigned a documented owner with an individual user identity
    d. Shall comply with the Access Controls Standard and Procedures
    e. May be subject to compensating security controls (e.g., limitation of permissions)

4. Service Accounts
    a. Shall be associated with application owners or a system administrator
    b. Shall be audited at least annually by ITS or at the direction of ITS
    c. Shall comply with the Access Control Standards and Procedures

5. System Administrator, Auditor, and Privileged Accounts
    a. System administrator(s) shall be documented in the approved ITS software asset inventory
    b. Administrator accounts shall be associated with active users.
        i. Credentials used to access information systems or network components ***shall not be defaults*** established by the manufacturer.
        ii. Default credentials from the manufacturer shall be changed, deleted, or otherwise disabled upon receipt and installation of the information system.
    c. Administrator accounts shall use multi-factor authentication where available
    d. System Administrators are responsible for the management of Privileged Accounts.
    e. User Access and Least Privilege Audits

i. Williamson County ITS shall ensure a review of users with administrative privilege on all ITS-managed information systems is conducted at least annually
ii. For non-ITS-managed information systems, department heads are responsible for annual review of users with administrative privilege to ensure compliance with least privilege.

Exceptions

Exceptions to technology-related policies, standards, and procedures 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 exception may require authorization by or consultation with Williamson County Human Resources, Purchasing, Facilities, Legal Counsel, Risk Management, Auditor's Office, Budget Office, or Commissioner's Court.

Violations

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 the temporary suspension or permanent revocation of user credentials and disciplinary action, up to and including termination of employment.

Related Policies, Titles, Forms, and Authorities

Acceptable Use Policy
Access Controls Standard and Procedures
Data Management Policy
Foreign Travel Notification Standard and Procedure
Foreign Travel Notification Form

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: Access Control

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

Revision History

Version	Date	Description
1.0		Policy Adoption by Williamson County Commissioners Court
0.1	10/25/22	First draft towards ITS GRC Engineering, CIS, NIST compliance with input from Human Resources, Risk Management, Legal Counsel