Williamson County Information Technology

Acceptable Use Policy - Technology

Sensitivity: None
Criticality: High
Primary Type: Policy

Summary

Purpose

The purpose of this policy is to establish acceptable parameters for use of all information systems authorized for deployment to provide public services and conduct county business and/or connected to Williamson County technology infrastructure.

Scope

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

Definitions

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.

Honeypot

A specially configured server, also known as a decoy server, designed to attract and monitor intruders in a manner such that their actions do not affect production systems.

Information System

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

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).

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 and Technology Services (ITS).

User

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

Workstation (Endpoint)
Refers to computers used by employees for business purposes. Typically, these will be Dell or Panasonic PC devices running Windows. Workstation and endpoint are used interchangeably.

Roles and Responsibilities

- Users are required to adhere to this policy while using any county information system.
- Users shall conduct themselves in a professional, responsible, and courteous manner at all times.
- Managers are required to inform all employees of this policy and ensure each employee understands and undertakes to comply with this policy.

Policy

This policy shall be referenced during Microsoft Windows log in to any county-managed computer. All County information systems are County property provided for the conducting of County business. Users shall be aware that communications, logs, data, or records collected, stored, or transmitted by information systems are subject to routine operational review, data breach investigations, or legal review as required by law.

A. Information Sharing and Confidentiality

Those within the scope of this policy shall:

1. Ensure release of county-related information to the public is in accordance with the Data Management Policy.
2. Comply with the Williamson County Access Control Policy and Data Management Policy.
3. Not read, view, or listen to other employees' electronic communications without a legitimate business need and appropriate permissions.
4. Be prudent and cautious when introducing audio, video, or software medium to an information system or device.
5. Be prudent and cautious when opening attachments or accessing links from within emails; and
6. Maintain current training in accordance with the Cybersecurity Awareness Training Policy.

B. Use of Internet

1. Except where expressly prohibited by a supervisor, limited personal use of county workstations is allowed when such activity does not impact either the user's assigned function or the security or privacy of the County's data. Users are expected to promote efficient use of information resources, consistent with County business objectives.
2. Users assume risks associated with accessing their personal accounts and information using county devices. ITS strongly recommends not saving personal information (bookmarks, passwords, etc..) on county-managed devices.
3. Williamson County reserves the right to restrict access to certain web locations.
4. Based on the business need to communicate with all County employees, only certain users have the authority to send electronic communications to all users.

5. Any elected official or department head may designate one or more individuals within their own department to send electronic communications to all employees within their own department even if the number of employees in that department exceeds the limit set by technical controls.

C. Security Controls

1. Passwords
    a. Passwords shall be created and maintained in accordance with Access Controls Standards and Procedures.
    b. Access to County systems and software is limited to authorized personnel with appropriate credentials. ITS requires security controls for user access to systems.
    c. Users shall not share work-related password information with anyone for any reason unless failure to do so presents a clear threat to life or property.
2. Hardware and Software
    a. Users shall ***immediately report loss, theft, destruction, or unauthorized use of County information systems or restricted / confidential information or potential compromise of information systems*** to their immediate supervisor or ITS in accordance with the Data Management Policy.
    b. ALL hardware connected to the County network or to a County computer (wired or wireless) must adhere to minimum security standards for Access Control and applicable policies and shall be assessed and validated by ITS for use. *For security reasons, some of these standards are Internal Use Only, and published to restricted audiences. Contact the ITS Service Desk for assistance with hardware evaluation and deployment.*
    c. ALL software introduced to county information systems including county mobile devices shall be centrally catalogued, even if the software is not maintained by ITS, to allow for audit against current threats / CVEs (Common Vulnerabilities and Exposures), and mitigation of threats reported by The MITRE Corporation, U.S. Department of Homeland Security, and / or the Cybersecurity and Infrastructure Security Agency (CISA).
    d. *Workstations shall not be used to copy non-work-related software from one storage medium to another*.
    e. Technical security controls for any peripheral connected to the county network or a county workstation shall be applied in accordance with currently adopted Standards and Procedures associated with County Access Controls and Data Management policies.
3. Training, Education, and Remediation
    a. ITS is responsible for ensuring compliance with mandates for **annual** cybersecurity awareness training in accordance with Texas state law.
    b. Cybersecurity Awareness Training is governed by the current County Cybersecurity Awareness Training Policy.
    c. Users are responsible for timely completion of required training related to information security in the performance of duties as a condition of continued access to county information systems.
    d. Users shall be accountable for activities and habits resulting in potential compromise of County information systems and shall be expected to remediate known behavioral errors

by education targeted to correct those errors (e.g., as result of controlled phishing tests / scenarios) as a condition of continued access to ITS managed information systems.

e. Elected officials and department heads (or their designees) are responsible for ensuring compliance with job-specific training requirements that may include content not present in annual cybersecurity awareness training (e.g., CJIS, FERPA, HIPAA, etc.).

D. Endpoint Management

1. ITS shall be responsible for making software security patches / updates available to users.
2. Users shall be responsible for allowing the installation of security and feature patches.
3. Critical software operating system patches shall be subject to requirement of installation within one (1) business day of being made available to end users.
4. **Under no circumstances shall unauthorized software be installed on or introduced to County information systems.**

E. Hostile Workplace

1. Abusive, harassing, bigoted, demeaning, obscene, and profane activities using any county-managed information system or device are strictly prohibited. These activities can result in criminal and/or civil liability or other penalties for the individual and the County.
2. Users or witnesses shall report any incidents of the sort listed in Section E, paragraph 1 of this policy immediately. Incidents should be reported to a supervisor or Human Resources.
3. Reports involving hostility in the workplace shall be referred to Human Resources with the full cooperation of ITS.

F. Violation Examples

Below are examples that are provided for context and understanding of this policy. This section is not meant to provide a comprehensive list of all possible unacceptable use.

1. Examples of **General** Violations
   a. Communications that violate the provisions of this policy
   b. Use of County resources for personal monetary gain
   c. Engaging in or enabling illegal activity using any County technology, including access to unlicensed copyrighted, pirated, or otherwise illicit materials
   d. Accessing, viewing, downloading, uploading, transmitting, printing, copying, posting, or sharing any racist, sexist, threatening, sexually explicit, obscene, or otherwise objectionable material (i.e., visual, textual, or auditory entity) is strictly prohibited.
   e. Unauthorized use of, access to, or disclosure of Confidential Information, as defined in federal or state law, or by the Data Management Policy
   f. Using County technology to create or contribute to an unsafe or hostile workplace
   g. Unauthorized provision of lists of or information about County employees or customers to parties outside of the County
   h. Introduction or injection or assisting in the introduction of malicious code or technology into the County network by negligence, malfeasance, or wonton disregard of County policy

i. Repurposing or disposal of a county device without appropriate sanitization of associated storage media, in accordance with County Data Management Policy and associated asset transfer standards

j. Careless positioning of display monitors in view of publicly accessible areas

k. **Posting or disclosure of sensitive or confidential information on social media.** For further clarification, please refer to Williamson County Data Management Policy for guidance on information release.

2. Examples of **System and Applications** Use Violations
   a. The posting of passwords in an area visible to those other than the user
   b. Introduction of any software to any county device without explicit consent by documented exception by ITS
   c. Circumvention of any authentication or security system
   d. Executing an undocumented change to a County information system outside of published change management standards or the technology trouble reporting system
   e. Performing break/fix troubleshooting of County information systems without appropriate documentation and communication to ITS management
3. Examples of **Network** Use Violations
   a. Connection of unauthorized devices to the County network, wired or wireless
   b. Conducting any unauthorized network communication activity, including:
      i. Use of accounts that are not the user's account
      ii. Installation of honeypots, honeynets, or similar tools unless those activities are defined within the user's job description and duties
      iii. Interference with or denial of service to any County information system management tools, unless those activities are defined within the user's job description and duties
      iv. Port or security scanning without direct and documented approval of the Chief Information Officer for Williamson County Information Technology (CIO) or designee.
4. Examples of **Email** Misuse
   a. Intentionally distributing spam, solicitations, or advertising material to individuals who did not request it
   b. Harassment of any kind
   c. Harvesting or attempting to harvest user credentials or protected information, unless as part of an ITS-sanctioned security assessment
   d. Misrepresentation of the County using County information systems

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 exceptions 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, software, and/or the user account from connection to Williamson County Information Systems or data. 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.

Malicious and egregious violations will result in immediate suspension of County IT assets and resources (step #3 below). Other types of violations will have the following progressive consequences based on a rolling 24-month time period.

1. **First violation:** The user must take an educational session in cooperation with Technology Services within two weeks. The educational session will be up to one hour in duration.
2. **Second violation:** The user will have their access to Williamson County IT assets and systems revoked until they have taken an in-depth education and remediation session in cooperation with Technology Services within two weeks. The session will be up to 8 hours in length. If the user cannot perform essential functions of their job without IT access, they may be required to utilize PTO or go on unpaid administrative leave until the successful completion of the education and remediation session.
3. **Third violation:** The user will have their access to Williamson County IT assets and systems revoked permanently unless an exception is granted by the County's Chief Information Officer. If an exception is requested and the user cannot perform essential functions of their job without IT access, they may be required to utilize PTO or go on unpaid administrative leave until the final determination of the exception request.

Related Statutes, Policies, and Authorities

Access Control Policy and Standards
Data Management Policy and Standards
Cybersecurity Awareness Training Policy
Policy Exception Standard and Procedure (via Employee Portal)

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: Acceptable Use Policy

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

Revision History

Version	Date	Description
3.0		Adoption by Commissioner's Court
2.1	02/27/2023	Violations section more precisely defined
2.0	01/17/2023	Adoption by Commissioner's Court
1.2	11/22/2022	Changes applied based on legal, HR, and risk management review. Prior version archived in DMS.
1.1	9/22/2022	Significant Changes applied. Updated for current county operations environment. Renamed to, "Acceptable Use Policy."
1	1/9/2008	First version. "Appendix B – Electronic Systems Use Policy