Williamson County Information Technology

Cybersecurity Awareness Training Policy

Sensitivity: None
Criticality: High
Primary Type: Policy

Summary

Purpose

Properly educating users about information security, best practices and risks serves to help reduce overall information security risks and probability of incidents. All users are required to complete Security Awareness Training to standards set by the State on an annual basis (in accordance with HB 3834). **Some users are required to complete additional training,** per Texas CJIS and the Department of State Health Services**. That additional training is not under the purview of Williamson County IT.**

Scope

This policy applies to all users of Williamson County Information Systems, as defined in this document.

Definitions

Department
Unless specifically noted otherwise, the use of the word "department" or related forms includes both Commissioners Court departments and all other 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.

Information System
Any hardware or software 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)

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

~~**Policy**~~

Roles and Responsibilities

- Williamson County is required to administer cybersecurity awareness training in accordance with state law.
- Users are responsible for completion of requisite training prior to the deadline.
- Department management is responsible for ensuring that users under their supervision have access to resources required to complete training.
- Departmental leaders or elected officials are responsible for ensuring compliance.

Policy

A. Regulatory Requirements

1. Texas HB 3834 requires ~~all Williamson County~~ information systems users to complete ~~state-certified~~ cybersecurity awareness training **on an annual basis**.
2. For Williamson County, the training requirement extends to vendors, contract and temp labor, and other applicable persons that access County data and the County computer network.
3. **ADDITIONALLY**, Texas Department of Public Safety (DPS) requires that all employees, contractors, and others with access to Texas Criminal Justice Information System (CJIS) data complete cyber security awareness at intervals defined by current CJIS Policy.
4. **ADDITIONALLY**, Texas Department of State Health Services (DSHS) requires that all employees and contractors with access to DSHS-regulated data take approved cyber security awareness training **on an annual basis**.
5. **Reporting**
   i. Williamson County IT shall report compliance to the Texas Department of Information Resources (DIR) annually.
   ii. Certification is required for certain grants. A current certificate of compliance shall be posted at a location accessible to employees from the County Employee 365 / SharePoint Portal

B. ~~Annual~~ Cybersecurity Awareness Training

1. Training in information security practices in use at Williamson County shall be provided by the county on an annual basis for all users.
2. Annual training shall be conducted online and in accordance with Texas HB 3834.
3. **Users that do not complete required training by published deadlines (see below) shall be subject to suspension of network and ITS-managed information system access.**
4. Supplemental training shall include monthly assessments using sanctioned phishing simulations
   i. Users who fail simulated phishing assessments will be required to complete remedial training
   ii. Users who do not complete remedial training are subject to account suspension

~~C. Periodic Assessment of Applied Knowledge~~

~~1. Ongoing training throughout the year shall include tactical attempts by authorized resources to assess practical compliance with training content (e.g., through authorized phishing scenarios, physical site visits, and controlled campaigns).~~

~~2. Remedial training will be required for those who do not pass sanctioned phishing assessments.~~

C. Timeframes and Deadlines

1. Annual Cybersecurity Awareness Training will open for all employees on or about February 1 each year
2. The deadline completion of ANNUAL cybersecurity awareness training shall be **May 31st** each year due to the effective date of Texas HB 3834. This accommodates legally required state reporting constraints.
3. New employees shall have access to training and assessment materials upon hire and are required to complete ~~the~~ training within ~~30 days~~ two (2) weeks of hire date.

D. Employee Communication

Aspects of communication with users includes:

1. Posting links to cybersecurity material on the Employee Portal and / or newsletters
2. Bi-annual email reminders to all employees by email and / or newsletters

E. Security Audits

Williamson County IT encourages all departments and users to audit their respective offices and work areas for application of acceptable security practices and compliance with county policies and standards. IT is available to consult or provide for any security audit services and report on the findings; as well as provide guidance for securing offices and workspaces.

Exceptions

Any exception must be documented, submitted to, and approved by the Williamson County CIO. Training requirements do not apply to employees and officials who, while the below conditions are applicable, have been:

1. Granted military leave
2. Granted leave under the Family and Medical Leave Act of 1993 (29 USC Section 2601 et seq)
3. Granted leave related to a sickness or disability covered by workers' compensation benefits, if that employee no longer has access to Williamson County Information Technology resources
4. Granted any other type of extended leave
5. Granted authorization to work from an alternative location if that employee no longer has access to Williamson County IT resources
6. Denied access to Williamson County's computer system or databases by the Williamson County Commissioners Court

Violations

Failure to complete required annual cybersecurity awareness training by the deadline shall result in limited access to the Williamson County network environment. These resources will only be fully restored when required training has been completed.

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

Consequences for failure of sanctioned phishing exercises shall be based on a rolling 24-month cycle and be handled in this manner:

1. **First failure**: Immediate feedback by means of a user-accessed landing page with descriptions of what a user may have not noticed to better identify a malicious email.
2. **Second failure**: Up to thirty-minute training session or repeat of Annual Cybersecurity Awareness Training.
3. **Third failure**: A third failure within the rolling 24-month period constitute a First Violation of the Williamson County Acceptable Use Policy.

Non-compliance with the legislation responsible for this policy (Texas HB 3834 and its amendments) may result in loss of grant funding from state resources and penalties to the county.

Related Statutes, Policies, and Authorities

Texas Government Code Title 10, B, 2054
Texas House Bill 3834. 86th Legislature. 2019

Administrative Revisions

This Policy may be revised by the Responsible Office or Department (see Administrative Notes) as necessary to add, delete, and modify procedural or administrative elements, as well as typographical corrections, without reapproval from the Commissioner's Court. All material changes to Policy scope, responsibilities, roles, intent, or other substantive changes must be formally approved by the Commissioner's Court. Any type of changes to this Policy must be posted to the County's Policy Management System and notes must be added to the Revision History section of this Policy.

Appendix

Training materials can be accessed via the Williamson County 365 Employee Portal.
https://wilco365.sharepoint.com/home

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: IT Cybersecurity Awareness Training

Responsible: ITS Director, GRC
Accountable: ITS CIO
Consulted: Gartner, Texas DIR, County Legal Counsel, HR, Elected Official
Informed: All Users with Attestation

Revision History

Version	Date	Description
4.0		Adoption by Williamson County Commissioners Court

3.3	1/23/2025	Periodic review Add section: Administrative Revisions B.4: Cadence of phishing assessment changed to monthly; remedial training is now mandatory C.2: Deadline changed to 3/31 annually C.3: Changed from 30 days after hire to 2 weeks after hire for new employee and returning employee security awareness training
3.2	6/17/2024	Apply 2024 template
3.1	02/20/2024	Rewording of violations sanctions section (reduced rolling 24-month cycle to static 12-month cycle) Change annual training deadline to March 31 Section B.4. Added requirement for phishing-specific awareness training for users who fail a sanctioned phishing campaign
3.0	03/21/2023	Adoption by Williamson County Commissioners Court
2.1	02/27/2023	Clarified progressive violations in Violations section, referencing Acceptable Use Policy.
2.0	01/17/2023	Adoption by Williamson County Commissioners Court
1.2	09/09/2022	Updated: Information from Texas HB 1118 (87R) exceptions added Added Roles and Responsibilities section (**Gartner** recommend) Requirements clarified: use of DIR-certified training materials Clarified deadlines appropriate to current state (DIR reporting) cycles Added this Revision History table
1.1	02/29/2022	Update to modern IT policy template
1.0	10/29/2019	Original adoption pursuant to Texas HB 3834