Williamson County Policy

Teleworking Policy

Approved Date: 7/20/2021
Approved By: Williamson County Commissioners Court
Last Revised: **7/12/2021**
Next Review: **7/19/2022**

Summary

Scope

This policy applies to all County employees who are permitted to telework by their department.

Purpose

If done properly, teleworking has been found to increase productivity for both the employee and the organization. With the appropriate tools and guidance, teleworking can be nearly seamless for the department. This policy defines the standards, eligibility, and other rules and requirements for teleworking.

Policy

1. Eligible Employees

a. The nature of the employee's work must allow for teleworking (doesn't require being physically present in the office).
b. The eligibility of an individual position is defined by the department head or elected official.
c. Performance and/or attendance issues (as defined by the supervisor) may affect an employee's eligibility to telework.
d. Violations of this policy may also affect an employee's eligibility to telework.
e. Departments may add other eligibility requirements as needed.

2. Remote Location Requirements

a. In order to telework, the remote location must have the appropriate setup for the employee be to effective, comfortable, and work securely for the duration of their shift.
b. It is the responsibility of the employee to provide the furniture, network connectivity, and other items needed to enable effective teleworking.

c. Certain software packages or processes may not perform as well from a remote location, and the employee and department may need to take this into account when authorizing telework.
d. Departments may define specific requirements, but generally, the remote location must allow the employee to work comfortably and safely for the duration of their shift.
e. If the employee cannot work effectively and securely from the remote location, teleworking may not be an option.

3. Technology Equipment

a. Employees are responsible for providing an internet connection sufficient to communicate (audio and video) with colleagues and/or customers as well as perform the needed tasks for their position from their telework location. The County will not provide MiFi devices for wireless internet for this purpose.
b. Employees are responsible for providing, testing, and validating the network connection before scheduling teleworking with their supervisor.
c. Any issues with personal (or public) network connectivity will be the responsibility of the employee to resolve or make alternate arrangements.
d. Employees must use County-owned computers or mobile devices to telework. This ensures compliance with County policies around hardware, security, and encryption.
e. Use of the County's Virtual Private Network (VPN) software is always required when accessing County data from an unsecured wireless or wired network.
f. Using personally owned devices (cell phones, iPads, etc.) for Office 365 applications is permitted but devices must comply with the security requirements below.
g. Generally, the County does not support equipment beyond computers and mobile devices at remote work locations.

4. Security

a. Utmost care must be taken to protect County data when working outside the office. This includes the physical placement of computer screens away from windows, unauthorized persons, or cameras.
b. Devices must not be left unattended at any time while unlocked.
c. There may also be regulations on the data, such as CJIS or HIPAA, that require additional security measures from working outside a secure location.
d. Supervisors are responsible for ensuring employees are compliant with all applicable regulations while teleworking.
e. Multi-Factor Authentication (MFA) is required to access data in Office 365 from a remote location. All teleworking employees must have the ability to receive a phone call or text message with a one-time use code when logging in from a new network location (on either a county phone number or cell phone). MFA is not applied when on the VPN. Additional controls or data security measures may apply depending on the nature of the work.

5. Technology Support

a. Technology Services will support users working remotely as much as possible but will not be able to support issues related to home/private internet issues, or personal equipment (routers, firewalls, etc.), as well as networked devices on non-County networks (e.g., network printers).
b. Technology Services will provide remote assistance to teleworking employees via phone, email, and remote support. No onsite support for teleworking employees is possible, so any issues that cannot be solved remotely will need to be done at IT or at another County office.

6. Communication Requirements

a. All teleworking employees must be reachable throughout their shift according to the standards set by their supervisor or department.
b. Communication methods that are supported by the County IT staff are email, Microsoft Teams, WebEx, and County phone.
c. Video chat/conferencing may be required depending on the position and nature of the work.

7. Performance Monitoring

a. Department heads and supervisors are responsible for determining the measurement of performance of teleworking employees as well as supervising staff while teleworking.
b. The criteria of performance will be clearly communicated to each employee before engaging in telework.
c. Employees may be asked to log into the County's timekeeping system or check in with a supervisor at the start and end/or of a teleworking shift depending on the position.
d. Performance monitoring may include computer logs, email and Teams messages, or other electronic means.
e. Failure to meet the performance criteria or policies may result in loss of eligibility to telework.

Related Policies, Titles, or Documents

Please refer to any department-specific policies that may reference this document.

Contact Office

Human Resources: Contact your designated HR representative or x31533
Technology Services: servicedesk@wilco.org or x31456

Revision History

Version	Date	Description
1	6/2/2020	First version – COVID-19 specific.
2	7/27/2021	Cleaned up language and made for more broad use cases