

# Montague County



## Prohibited Technologies Security Policy

Date: August 28, 2023

## TABLE OF CONTENTS

---

<b>Table of Contents .....</b>	<b>2</b>
<b>1.0 Introduction .....</b>	<b>3</b>
1.1 Purpose .....	3
1.2 Scope.....	3
<b>2.0 Policy.....</b>	<b>3</b>
2.1 County-Owned Devices.....	3
2.2 Personal Devices Used For County Business .....	4
2.3 Identification of Sensitive Locations .....	4
2.4 Network Restrictions .....	5
2.5 Ongoing and Emerging Technology Threats .....	5
<b>3.0 Policy Compliance .....</b>	<b>5</b>
<b>4.0 Exceptions .....</b>	<b>6</b>
<b>Addendum A .....</b>	<b>7</b>
<b>Acknowledgement.....</b>	<b>8</b>
<b>Device Compliance .....</b>	<b>9</b>

## 1.0 INTRODUCTION

---

### 1.1 PURPOSE

On December 7, 2022, Governor Greg Abbott required ([https://gov.texas.gov/uploads/files/press/State\\_Agencies\\_Letter\\_1.pdf](https://gov.texas.gov/uploads/files/press/State_Agencies_Letter_1.pdf)) all state and county agencies to ban the video-sharing application TikTok from all government-owned and government-issued devices and networks over the Chinese Communist Party's ability to use the application for surveilling Texans. Governor Abbott also directed the Texas Department of Public Safety (DPS) and the Texas Department of Information Resources (DIR) to develop a plan providing state and county agencies guidance on managing personal devices used to conduct government business.

In addition to TikTok, **Montague County** may add other software and hardware products with security concerns to this policy and will be required to remove prohibited technologies which are on the DIR prohibited technology list. Throughout this Policy, "Prohibited Technologies" shall refer to TikTok and any additional hardware or software products added to this Policy.

### 1.2 SCOPE

This policy applies to all **Montague County** full and part-time employees including contractors, paid or unpaid interns, and users of county networks. All **Montague County** employees are responsible for complying with the terms and conditions of this policy.

## 2.0 POLICY

---

### 2.1 COUNTY-OWNED DEVICES

Except where approved exceptions apply, the use or download of prohibited applications or websites is prohibited on all county-owned devices, including cell phones, MiFis, tablets, desktop and laptop computers, and other internet capable devices.

**Montague County** must identify, track, and control county-owned devices to prohibit the installation of or access to all prohibited applications. This includes the various prohibited applications for mobile, desktop, or other internet capable devices.

**Montague County** must manage all county-issued mobile devices by implementing the security controls listed below:

- a. Restrict access to “app stores” or non-authorized software repositories to prevent the install of unauthorized applications.
- b. Maintain the ability to remotely wipe non-compliant or compromised mobile devices.
- c. Maintain the ability to remotely uninstall un-authorized software from mobile devices.
- d. Deploy secure baseline configurations, for mobile devices, as determined by **Montague County**.

## 2.2 PERSONAL DEVICES USED FOR COUNTY BUSINESS

Employees and contractors may not install or operate prohibited applications or technologies on any personal device that is used to conduct county business. County business includes accessing any county-owned data, software, applications, email accounts, non-public facing communications, county email, VoIP, SMS, video conferencing, CAPPs, Texas.gov, and any other county databases or applications.

If an employee or contractor has a justifiable need to allow the use of personal devices to conduct county business, they may request that their device be enrolled in the agency’s “Bring Your Own Device” (BYOD) program.

## 2.3 IDENTIFICATION OF SENSITIVE LOCATIONS

Sensitive locations must be identified, cataloged, and labeled by the agency. A sensitive location is any location, physical, or logical (such as video conferencing, or electronic meeting rooms) that is used to discuss confidential or sensitive information, including information technology configurations, criminal justice information, financial data, personally identifiable data, sensitive personal information, or any data protected by federal or state law.

Unauthorized devices such as personal cell phones, tablets, or laptops may not enter sensitive locations, which includes any electronic meeting labeled as a sensitive location.

Visitors granted access to secure locations are subject to the same limitations as contractors and employees on unauthorized personal devices when entering secure locations.

## 2.4 NETWORK RESTRICTIONS

DIR has blocked access to prohibited technologies on the state network. To ensure multiple layers of protection, **Montague County** will also implement additional network-based restrictions to include:

- a. Configure agency firewalls to block access to statewide prohibited services on all agency technology infrastructures, including local networks, WAN, and VPN connections.
- b. Prohibit personal devices with prohibited technologies installed from connecting to agency or county technology infrastructure or county data.
- c. Provide a separate network for access to prohibited technologies with the approval of the executive head of the agency.

## 2.5 ONGOING AND EMERGING TECHNOLOGY THREATS

To provide protection against ongoing and emerging technological threats to the state's sensitive information and critical infrastructure, DPS and DIR will regularly monitor and evaluate additional technologies posing concerns for inclusion in this policy.

DIR will host a site that lists all prohibited technologies including apps, software, hardware, or technology providers. The prohibited technologies list current as of January 23, 2023, can be found at Addendum A. New technologies will be added to the list after consultation between DIR and DPS.

**Montague County** will implement the removal and prohibition of any listed technology. **Montague County** may prohibit technology threats in addition to those identified by DIR and DPS.

## 3.0 POLICY COMPLIANCE

---

All employees shall sign a document annually confirming their understanding of this policy.

Compliance with this policy will be verified through various methods, including but not limited to, IT/security system reports and feedback to agency leadership.

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

## 4.0 EXCEPTIONS

---

Exceptions to the ban on prohibited technologies may only be approved by the Commissioner's Court of **Montague County**. This authority may not be delegated. All approved exceptions to the TikTok prohibition or other statewide prohibited technology must be reported to DIR.

Exceptions to the policy will only be considered when the use of prohibited technologies is required for a specific business need, such as enabling criminal or civil investigations or for sharing of information to the public during an emergency. For personal devices used for county business, exceptions should be limited to extenuating circumstances and only granted for a pre-defined period of time. To the extent practicable, exception-based use should only be performed on devices that are not used for other county business and on non-county networks. Cameras and microphones should be disabled on devices for exception-based use.

## ADDENDUM A

---

The up-to-date list of prohibited technologies is published at <https://dir.texas.gov/information-security/prohibited-technologies>. The following list is current as of January 23, 2023.

### **Prohibited Software/Applications/Developers**

- TikTok
- Kaspersky
- ByteDance Ltd.
- Tencent Holdings Ltd.
- Alipay
- CamScanner
- QQ Wallet
- SHAREit
- VMate
- WeChat
- WeChat Pay
- WPS Office
- Any subsidiary or affiliate an entity listed above.

### **Prohibited Hardware/Equipment/Manufacturers**

- Huawei Technologies Company
- ZTE Corporation
- Hangzhou Hikvision Digital Technology Company
- Dahua Technology Company
- SZ DJI Technology Company
- Hytera Communications Corporation
- Any subsidiary or affiliate an entity listed above.

## PROHIBITED TECHNOLOGIES SECURITY POLICY ACKNOWLEDGEMENT

---

I have received a copy of the Montague County Prohibited Technologies Security Policy that outlines Montague County's ban on prohibited technologies, including TikTok, from all county-owned devices and networks. I understand that the use or download of prohibited applications or websites is prohibited on all county-owned devices, including cell phones, MiFis, tablets, desktop and laptop computers, and other internet capable devices. I understand that I may not install or operate prohibited applications or technologies, including TikTok, on any personal device that is used to conduct county business, including accessing county e-mail accounts. I further understand that any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

I understand that I am responsible for reading and familiarizing myself with the information in this policy. If I need clarification on any of the information in this policy, I will contact my immediate supervisor.

I have read the Montague County Prohibited Technologies Security Policy and I agree to comply with the terms and conditions of this policy.

---

Printed Name of Employee

---

Signature of Employee

---

Date Signed



## DEVICE COMPLIANCE

---

Please choose from the following options:

- I have been issued a county-owned device, including cell phone, MiFi, tablet, desktop or laptop computer, or other internet capable device.
  - I certify that all prohibited technologies, including TikTok, have been removed from my county-owned device and will not be used or downloaded on such device in the future.
  
- I use my personal device, including cell phone, MiFi, tablet, desktop or laptop computer, or other internet capable device to conduct county business or check county email. County business includes accessing any county-owned data, software, application, or email.
  - I certify that all prohibited technologies, including TikTok, have been removed from my personal device and will not be used or downloaded on such device, at home or at work, while using my personal device to conduct county business or check county email.
  - or-
  - I certify that I have removed all county e-mail from my personal device and will not use my personal device to conduct county business in the future while having prohibited technologies installed on my personal device.
  
- I do not have a county-owned device nor do I use my personal device to conduct county business.

I understand that a violation of this policy may result in disciplinary action, up to and including termination of employment.

---

Printed Name of Employee

---

Signature of Employee

---

Date Signed

**COUNTY OF MONTAGUE  
COMMISSIONER'S COURT ORDER**

WHEREAS the Montague County Commissioner's Court desires to preserve the safety and security off all Montague County's sensitive information and to protect itself from the Chinese Communist Party as directed by Governor Greg Abbott on December 7, 2022; and


WHEREAS the Montague County Commissioner's Court wish to adequately communicate to employees the policies and procedures of the County:

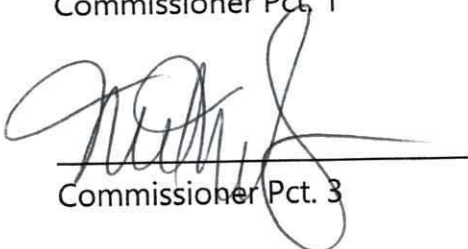
THEREFORE, BE IT RESOLVED that the Montague County Commissioner's Court hereby approve, and adopt, the MONTAGUE COUNTY PROHIBITED TECHNOLOGIES SECURITY POLICY.

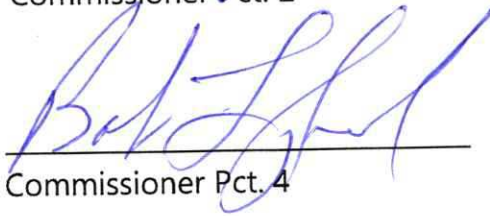
ADOPTED THIS 23<sup>TH</sup> DAY OF AUGUST, 2023

  
\_\_\_\_\_  
County Judge

\_\_\_\_\_  
Commissioner Pct. 1

  
\_\_\_\_\_  
Commissioner Pct. 2

  
\_\_\_\_\_  
Commissioner Pct. 3

  
\_\_\_\_\_  
Commissioner Pct. 4

Witnessed and Attested By:

  
\_\_\_\_\_  
County Clerk



**RESOLUTION FOR MONTAGUE COUNTY**

I the undersigned have read the Montague County Prohibited Technologies Security Policy that the Montague County Commissioner's Court has adopted. As an ELECTED OFFICIAL of Montague County, I endorse and approve the Prohibited Technologies Security Policy. I approve the document as it reflects my commitment to Montague County employees, and it reflects my commitment to conform to appropriate state and federal laws.

I agree to be bound by the terms and conditions of the Montague County Prohibited Technologies Security Policy, as witnessed by my signatures below.

---

Printed Name of Elected Official

---

Office of Elected Official

---

Signature of Elected Official

---

Date Signed