Clarendon College

Prohibited Technologies Security Policy

Date: January 31, 2025

Version: 1.2

TABLE OF CONTENTS

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) all state agencies to ban the video-sharing application TikTok from all state-owned and state-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 to guide state agencies on managing personal devices used to conduct state business.

In addition to TikTok, **Clarendon College** may add other software and hardware products with security concerns to this policy and will be required to remove prohibited technologies 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 **Clarendon College** full and part-time employees, including contractors, paid or unpaid interns, and users of state networks. All **Clarendon College** employees are responsible for complying with the terms and conditions of this policy.

2.0 POLICY

2.1 STATE-OWNED DEVICES

Except where approved exceptions apply, the use or download of prohibited applications or websites is not permitted on all state-owned devices, including cell phones, tablets, desktop and laptop computers, and other internet-capable devices.

The **Clarendon College** must identify, track, and control state-owned devices to prohibit the installation of or access to all banned applications. This includes the various prohibited applications for mobile, desktop, or other internet-capable devices.

The **Clarendon College** must manage all state-issued mobile devices by implementing the security controls listed below:

a. Restrict access to "app stores" or non-authorized software repositories to prevent unauthorized applications from being installed.
b. Maintain the ability to wipe non-compliant or compromised mobile devices remotely.
c. Maintain the ability to uninstall unauthorized software from mobile devices remotely.
d. Deploy secure baseline configurations for mobile devices, as determined by **Clarendon College**.

2.2 Personal Devices Used For State Business

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

Suppose an employee or contractor has a justifiable need to allow personal devices to conduct state business. In that case, they may request that their device be enrolled in the agency's "Bring Your 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, **Clarendon College** 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 from being installed and connected to agency or state technology infrastructure or 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 protect 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, and technology providers. The prohibited technologies list current as of January 23, 2023, can be found in Addendum A. New technologies will be added to the list after consultation between DIR and DPS.

Clarendon College will implement the removal and prohibition of any listed technology. **Clarendon College** 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, including termination of employment.

4.0 EXCEPTIONS

Exceptions to the ban on prohibited technologies may only be approved by the executive head of **Clarendon College**. 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 prohibited technologies are required for a specific business need, such as enabling criminal or civil investigations or sharing information with the public during an emergency. For personal devices used for state business, exceptions should be limited to extenuating circumstances and only granted for a pre-defined period. To the extent practicable, exception-based use should only be performed on devices not used for other state business and non-state networks. Cameras and microphones should be turned off on devices for exception-based use.

5.0 VERSION HISTORY

This table summarizes the significant edits, i.e., edits affecting transition points, process changes, system changes, and/or role changes.

Version	Date	Responsible	Revision Summary
1.0	January 26, 2023	Name	Document Creation

6.0 Related Policies, References, and Attachments:

An index of approved Clarendon College-IT policies can be found on the Clarendon College Information Technology Services Policies website at https://www.clarendoncollege.edu/information-technology. The Policy Compliance Document contains reference materials, legal compliance guidelines, and policy enforcement. The Clarendon College Information Security Program and Clarendon College Information Security User Guide are also available on the Information Technology Services Policies website.

The Clarendon College Board of Regents approved this policy on July 17, 2023, version 1.1. This policy was reviewed by Will Thompson, Vice President of IT, on July 15, 2023.

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
- RedNote
- DeepSeek
- Webull
- Tiger Brokers
- Moomoo
- Lemon8
- Any subsidiary or affiliate of 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 of an entity listed above.

The Clarendon College Board of Regents approved this policy on March 27, 2027, version 1.2.
This policy was reviewed by Will Thompson, Vice President of IT, on February 18, 2025.