TEXAS WORKFORCE COMMISSION
Workforce Development Letter

ID/No:	WD 29-22, Change 2
Date:	April 25, 2023
Keyword:	Administration
Effective:	Immediately

To: Local Workforce Development Board Executive Directors
Commission Executive Offices
Integrated Service Area Managers

From: Courtney Arbour, Director, Workforce Development Division

Subject: **Ban of TikTok and Other Nonwork-Related Social Network Services—Update**

PURPOSE:

The purpose of this WD Letter is to provide Local Workforce Development Boards (Boards) with guidance on banning and removing TikTok and other nonwork-related social network services on government-issued devices or devices used to access Texas Workforce Commission's (TWC) information and systems.

This change letter provides updated guidance on requirements related to prohibited technologies and the use of personal devices, including prohibiting the use of technology-enabled personal devices with prohibited technologies to conduct state business and access TWC information and systems.

RESCISSIONS:

WD Letter 29-22, Change 1

BACKGROUND:

On December 7, 2022, Governor Greg Abbott directed every state agency in Texas to ban its officers and employees from downloading or using TikTok on any government-issued devices, including cell phones, laptops, tablets, desktop computers, and other devices capable of internet connectivity. TikTok is a video-sharing mobile application that has been determined to be a potential security issue for any entity using it.

On February 6, 2023, the governor announced the statewide model security plan for prohibited technologies developed by the Texas Department of Public Safety (DPS) and the Texas Department of Information Resources (DIR) and directed state agencies to implement their own policies by February 15, 2023. TWC has adopted the Prohibited Technologies Security Policy to align with the guidance from the governor.

TWC Information Security Manual §3.2.18, Internet Content Filtering, requires TWC to have an internet filtering system that blocks access to websites and protocols that are deemed inappropriate for the agency's environment, including social network services.

Agency Board Agreement (ABA), Attachment C, Board Guidelines for Security, provides guidelines for the minimum acceptable standards for the Texas Cybersecurity Framework control objectives to ensure the security of TWC data entrusted to each Board.

PROCEDURES:

No Local Flexibility (NLF): This rating indicates that Boards must comply with the federal and state laws, rules, policies, and required procedures set forth in this WD Letter and have no local flexibility in determining whether and/or how to comply. All information with an NLF rating is indicated by "must."

Local Flexibility (LF): This rating indicates that Boards have local flexibility in determining whether and/or how to implement guidance or recommended practices set forth in this WD Letter. All information with an LF rating is indicated by "may" or "recommend."

LF: Boards may adopt policies to implement the requirements related to prohibited technologies, Board-issued devices, and personal devices.

Prohibited Technologies

NLF: Boards must be aware that DPS and DIR will evaluate and monitor technologies that pose a threat to state sensitive information and critical infrastructure. DIR will maintain an up-to-date list of prohibited technologies and provide recommendations to state leaders on technologies that must be blocked. The list of prohibited technologies is available on DIR's website.

Board-Issued Devices

NLF: Boards must ban the use of TikTok and all other prohibited technologies on all Board-issued systems and devices, as Boards have access to sensitive material that could potentially be made available to those databases. If TikTok or any other prohibited technology is currently installed on any such devices, it must be removed immediately.

NLF: Boards must configure firewalls to block access to statewide prohibited technologies on all Board technology infrastructures, including local networks, WAN, and VPN connections.

Technology-Enabled Personal Devices

NLF: Boards must be aware that "technology-enabled personal devices," also referred to as "personal devices" in this letter, are defined as a cell phone, laptop, tablet, desktop computer, or any other device capable of internet connectivity.

NLF: Boards must adopt one of the following options related to personal devices:

- Implement a "Bring Your Own Device" policy and mobile device management platform that complies with the considerations in objective #2 of the Statewide

Plan for Preventing Use of Prohibited Technologies; or

- Prohibit the use of personal devices to conduct business related to TWC programs, including accessing any state or board-owned data, applications, nonpublic facing communications, and email accounts.

NLF: Boards that implement a "Bring Your Own Device" policy must submit that policy to ciso@twc.texas.gov for approval.

LF: Boards may allow the use of MiFi devices or other cellular wireless hotspots, as these devices cannot download prohibited software.

NLF: Boards must prohibit the use of personal cellular smartphones or other smart devices as mobile hotspots for connecting to Board systems, as these devices can download prohibited software, unless the device has been approved through the "Bring Your Own Device" policy.

Sensitive Locations

NLF: Boards must identify, catalog, and label sensitive locations within Board and contractor offices by February 28, 2023. Aside from the guidance provided immediately below, a sensitive location may be determined to be 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, and/or any data protected by federal or state law.

NLF: Boards must be aware of the following regarding sensitive locations:

- Workforce Solutions Offices are already designed to protect the confidentiality of sensitive information, in accordance with WD Letter 02-18, issued March 23, 2018, and titled "Handling and Protection of Personally Identifiable Information and Other Sensitive Information."
- All Workforce Solutions Offices should have some areas that are not designated as sensitive locations. These areas could include resource rooms, restrooms, cubicles, and public meeting spaces.
- Boards must not prohibit individuals from bringing personal devices into public areas.
- Boards must ensure that technology-enabled personal devices are not allowed in any sensitive location.
- Public Board meetings must not be considered sensitive locations. Boards must not restrict access to personal devices—even devices with prohibited technologies—during public Board meetings.

INQUIRIES:

Send inquiries regarding this WD Letter to wfpolicy.clarifications@twc.texas.gov.

ATTACHMENTS:

Attachment 1: State Agencies Letter
Attachment 2: TWC Prohibited Technologies Security Policy

Attachment 3: Revisions to WD Letter 29-22, Change 1, Shown in Track Changes

REFERENCES:

TWC Information Security Manual, Version 3.0
DIR List of Prohibited Technologies
Agency Board Agreement, Attachment C—Board Guidelines for Security