Standards for Technologies Prohibited by Regulation

Purpose

This standard establishes (1) a non-exhaustive record of technologies and technology service providers from which the Institute is prohibited from using and/or acquiring and (2) a non-confidential explanation of technical and administrative controls implemented in the furtherance of related compliance goals. Prohibitions highlighted in this standard correspond to state and federal laws, directives, executive orders, and other regulatory requirements applicable to the Institute. The absence of an otherwise prohibited item from this Standard does not imply a means by which the item is authorized.

The contents of this standard are additive overlays that incorporate, detail, and extend requirements set by the TSUS Information Technology Policies, institutional policies, other institutional standards, procedures, and guidelines, and additional prohibitions, such as the “Debarred Vendor List” maintained by the Texas Comptroller of Public Accounts.

Pursuant to section 552.139 of Texas Government Code (“Public Information”), some descriptions of technical security controls, procedures, and practices will be abbreviated to avoid disclosure of confidential information pertaining to the security posture of the Institute’s information resources.

Scope

This standard generally applies to all Institute-owned information systems, devices,

networks, and other information resources that are within the custodianship of the Institute regardless of location. As detailed within, certain sections of this standard may also be applicable to Institute personnel (e.g., Institute officers, employees, contractors), locations (e.g., campuses, properties), and personally owned devices (e.g., those used to conduct state or Institute business).

Summary

This section provides an overview of the requirements of this standard. This summary is provided for reference purposes and does not take the place of the full text below.

- All Institute employees are prohibited from downloading or using TikTok on any Institute device or other information resource. Similarly, the installation or use of TikTok on any Institute owned device or other information source is prohibited by any user. Exceptions to this prohibition may only be granted by the Institute's president.

Publication and Updates

This standard was first published on 12/9/2022. This section will be updated when any updates or changes are made to this standard.

Definitions

Terms used in this standard have the meaning ascribed in the Information Security Glossary unless otherwise clarified in this section.

- ***DIR.*** Initialism for the Texas Department of Information Resources
- ***DPS.*** Initialism for the Texas Department of Public Safety
- ***Institutional User.*** A privileged or non-privileged user of an information system who holds an active affiliation (e.g., faculty, staff, student) with LIT.
- ***ISO.*** Initialism for LIT's "Information Security Office"
- ***Logical Device.*** Logical equivalents of Devices, such as virtual Servers and virtualized versions of Networks
- ***Non-privileged User.*** See "User"
- ***OOG.*** Initialism for the Texas Office of the Governor
- ***Organizational User.*** See "Institutional User"

Exceptions to this Standard

The feasibility of exceptions to this standard and processes by which such exceptions

may be facilitated will be detailed within the body of this document. Unlike certain security controls, policies, standards, and other requirements of the Institute, the regulatory nature of the prohibitions described by this standard significantly limit or prevent exceptions from being granted by the Institute's agency head, information security officer, individual department heads, or other Institute personnel.

Appropriate Use of Information Resources

Users of Institute information resources are subject to the requirements set by Institute policy, including Policy 2.11 Appropriate Use of Information Technology. Requirements set by this policy include, but are not limited to, the following summary:

- 4.6 Employees of LIT are allowed to use LIT‘s information resources in the performance of their job duties as long as they adhere to all applicable policies and statutes. Incidental personal use of information resources by an employee is permitted, subject to review and reasonable restrictions by the employee‘s supervisor. Such personal use must not violate any applicable policies and statutes, must not interfere with the employee‘s job performance, and must not result in any additional expense to LIT.

Per section 5 Inappropriate Uses of Information Resources, prohibited activities for all users include, but are not limited to, the following:

- 5.1.2 Failure to comply with laws, policies, procedures, license agreements, and contracts that pertain to and limit the use of the LIT‘s information resources, and
- 5.1.10 Participating or assisting in the deliberate circumvention of any security measure or administrative access control that pertains to LIT information resources.

Prohibition of TikTok [12/7/22 Texas OOG Executive Order]

REGULATORY SOURCE

This prohibition stems from an OOG executive order issued on 12/7/22. As stated in the letter sent to state agency heads,

> "…effective immediately, every state agency in Texas shall ban its officers and employees from downloading or using TikTok on any of its government-issued devices. This TikTok ban extends to all state-issued cell phones, laptops, tablets, desktop computers, and other devices capable of internet connectivity, and it must be strictly enforced by your agency's IT department."

For further information, see the following pages:

- https://gov.texas.gov/news/post/governor-abbott-orders-aggressive-action-against-tiktok
- https://gov.texas.gov/uploads/files/press/State_Agencies_Letter_1.pdf

PROHIBITION

Effective 12/7/22, all Institute employees are prohibited from downloading or using TikTok on any Institute-owned or Institute-issued devices and other Institute information resources. Further, the installation or use of TikTok on Institute-owned or Institute-issued devices and other Institute information resources by any user, including contractors, students, sponsored student organizations, and non-affiliates, is prohibited.

EXCEPTIONS TO THIS PROHIBITION

Pursuant to the executive order, exceptions to this prohibition may be made with authorization from the Institute's president as the designated state agency head. As

stated in the letter sent to state agency heads,

> "As head of your agency, you may grant exceptions to enable law-enforcement investigations and other legitimate uses of TikTok on state-issued devices. This authority may not be delegated. These narrow exceptions must be reported to the Office of the Governor (OOG)."

As of 12/9/2022, the following scenarios have been approved by the Institute president:

1. Cybersecurity incident investigations
2. Dean of Students investigations
3. Title IX investigations
4. Legal Discovery
5. Temporary maintenance of dormant, high value TikTok handles to reduce risk of impersonation

TECHNICAL CONTROLS

In response to this prohibition of the use of the TikTok social media service on Institute-owned devices, a series of technical controls will be used. Technical controls include, but may not be limited to, the following:

- Blocking the use of TikTok software and access to TikTok services on Institute-managed endpoints via technology-based controls
- Blocking access to TikTok from all parts of the Institute network

ADMINISTRATIVE CONTROLS

Measures that have or will be taken include, but may not be limited to, the following:

- Issuance of this standard

- Removal of content on Institute webpages referencing and/or linking to TikTok other than those used to communicate and facilitate compliance with the order such as this standard
- Reviews of institutional procurement activity to assess direct spending with TikTok
- Identification and neutralization of TikTok accounts controlled by the Institute and external parties on behalf of the Institute
- Communication to multiple stakeholder groups
- Establishing and appropriately reporting exceptions authorized by the Institute president

PROCEDURES TO DISABLE TIKTOK ACCOUNTS

Prior to the 12/7/22 executive order, parts of the Institute used TikTok as a component of social media strategies. In order to mitigate the likelihood of username reclamation and subsequent impersonation by threat actors, the following procedures are to be implemented by the respective information resource owner and information resource custodian of Institute-managed TikTok accounts:

1. Archive copies of content posted to the account and store the archived copies in an authorized location (e.g., Institute fileshare, SharePoint) in compliance with the records retention schedule
2. Remove all content from each account
3. De-brand each account by removing all institutional logos, contact information, and similar details
4. Leave the account active and maintain it under LIT control
5. Remove any remaining instances of TikTok applications from Institute-owned

devices

6. Confirm the account has been registered with the Information Security department and do not use it further

Additional procedures may include temporarily logging on to the account from an authorized source to prevent deactivation of the account and loss of the account's reserved username after a period of approximately 170 days of inactivity. These procedures may be activated based on several factors, including risk analysis, shifts in the threat landscape, and the status of authorized exceptions.