

Technologies Prohibited by Regulation FAQ

General Questions

What's the difference between a Covered Application and a Prohibited Technology?

	Covered Applications	Prohibited Technologies
Scope	Limited to certain social media applications and services (e.g., TikTok, Lemon8, RedNote).	Encompasses a broad set of software and hardware products and services.
Application	Prohibition only applies to Institute-owned computers and mobile devices.	Broad set of technical and administrative requirements.
Exceptions	Exceptions are extremely limited. Law enforcement and Information Security Measures only. The Institute has no authority to make exceptions.	Limited exceptions can be authorized by the Institute President.

Can I request an exception to access a technology prohibited by the Governor's directive?

Faculty and staff may request exceptions for Prohibited Technologies. To request an exception, complete the Exception Request Form. The form must include a business justification and be approved by the President. See Standards for Technologies Prohibited by Regulation for more information.

Note: No exceptions may be authorized for social media services classified as Covered Applications under [Texas Government Code §620](#).

What's a mobile device?

For this policy, mobile devices include but are not limited to laptops, smart phones, tablets, smart watches, and e-readers.

What technologies are prohibited?

The DIR maintains a list of Prohibited Technologies and Covered Applications, including software, applications, developers, hardware, equipment, and manufacturers, as well as technologies from any subsidiary or affiliate of an entity on DIR's list (e.g., a software studio or child company partially owned by a listed entity).

More information regarding Prohibited Technologies and Covered Applications can be found on the [DIR Covered Applications and Prohibited Technologies webpage](#).

Can I access TikTok (or other prohibited software) on LIT property as long as I'm using a personal device and my own data?

LIT does not manage user's personal devices. Users with personal devices with prohibited technologies installed will be prohibited from entering sensitive locations and blocked on the Institute network if they connect to Institute-owned networks.

Why does LIT have to comply with the Governor's Directive on Prohibited technologies?

LIT is a public Institute and a state agency and is therefore subject to complying with requirements set by the Office of the Governor, rules set by regulatory agencies, and legislative mandates passed into law. Further, the Texas State University System issues policies corresponding to similar compliance requirements.

Students

I'm a student, not an employee, so why do these rules even apply to me?

These rules apply to all individuals accessing Institute-owned information resources.

I'm a student employee at LIT. If other students can have TikTok on their personal devices, why can't I?

You may have prohibited technologies on personally-owned devices. However, you cannot conduct Institute business from a personally-owned device that contains prohibited technologies.

Can I access prohibited technologies if I live in Institute housing?

Yes, an exception has been granted for students who live in Institute housing and connect their personal devices to the Institute residential network via wireless or ethernet connection. Devices connected to the other Institute wireless networks are not included in this exception.

My student organization has a TikTok account. Do we have to delete it?

Sponsored student organizations should report use of prohibited technologies by completing the Institute's [Information Security Incident Form](#).

Faculty and Staff

I'm a faculty member at LIT teaching a course that uses a prohibited technology. What do I do?

Let us know the use of your prohibited technology by completing the Institute's [Information Security Incident Form](#) and representatives from Information Technology Services will contact you with recommendations on next steps.

I'm a faculty/staff member, how does this impact my day-to-day?

This answer depends on the tools and technologies you use on a day-to-day basis. Employees who use only Institute-owned devices, software, and other technologies to do their job should experience little to no impact.

What do I do if I currently use a prohibited technology for Institute business?

Discontinue the use of the prohibited technology and let us know by completing the Institute's [Information Security Incident Form](#). Representatives from Information Technology Services will contact you with recommendations on next steps.

I'm an employee and I have a prohibited technology on my personal mobile device. May I continue to check my LIT email, access the VPN, or log on to Blackboard, Banner, or other Institute systems from this device?

No. Having prohibited technology on your personal device while conducting state business is prohibited. You need to remove the prohibited technology before continuing to use this device for Institute business. If you are required to conduct Institute business on this device and cannot or will not remove the prohibited technology, you should consult with your supervisor about what device(s) may be made available for performing your duties.

Is my home considered a sensitive location when working with Institute data?

No. Sensitive locations will be designated by LIT and will be marked as such.

I'm an employee using my personal device to work remotely. May I continue to do so?

It is recommended that an Institute-issued device be used to work remotely. However, if a personal device is being used to conduct Institute business, prohibited technologies cannot be installed.

Is my home network now prohibited from allowing devices with prohibited technology from connecting to it?

No. Requirements for network restrictions are limited to Institute-owned networks.

I have a personal device with prohibited technologies installed, can I respond to Duo notifications or calls to log on to my LIT accounts?

Yes, within the scope of this prohibition, using your personal device as part of Duo Multi-Factor Authentication (MFA) is not considered conducting state business or Institute business.

I'm an LIT employee using my personal cell phone to text or call my coworkers about non-confidential work-related items. Is this allowed?

Yes, you are allowed to use your personal device to call or text your coworkers to conduct Institute business if you are not transmitting sensitive or confidential information.

I use my personal device to check my LIT email. Does it have to be enrolled in the Institute's device management software?

No. LIT's device management software is for Institute-owned devices.

I'm trying to purchase computing hardware or software and I want to make sure it is compliant. Where do I go to check?

The DIR maintains a list of prohibited technologies, including software, applications, developers, hardware, equipment, and manufacturers, as well as technologies from any subsidiary or affiliate of an entity on DIR's list (e.g., a software studio or child company partially owned by a listed entity). As part of the IT procurement process, Information Security and Information Technology Services will perform reviews that include a prohibited technology check.

More information regarding Prohibited Technologies and Covered Applications can be found on the [DIR Covered Applications and Prohibited Technologies webpage](#).

[View the IT Procurement Procedures](#)