Export Controls & Prohibited Technology

AnSRS4U

June 26, 2025

10:00-11:00am

RESPONSIBLE CONDUCT OF RESEARCH CREDIT

To receive RCR credit for today's presentation, please email RCR@tamu.edu with your name, UIN, and notification that you attended this presentation.

Upcoming RCR Sessions:

- **Tuesday, July 1, 2025– 1 hour - Virtual**
  - 10:00-11:00am– RCR – Export Controls
- **Wednesday, July 16, 2025– 1 hour - Virtual**
  - 10:00-11:00am – RCR – Biosafety
- **Thursday, August 21, 2025– 4 hours – In Person (must attend all 4 hours)**
  - 10:00am-2:30pm:
    - Research Data Management
    - Research Security
    - Safe Research Environments
    - Research Misconduct, Authorship & Peer Review
- **Thursday, October 23, 2025– 1 hour - Virtual**
  - 10:00-11:00am – RCR – Animal Welfare
- **The following workshops are available year-round through other departments/offices:**
  - Research Data Management courses – taught through University Libraries
  - Mentor/Mentee courses – taught through the Graduate Mentoring Academy
  - RCR – Lab Specific Training – training provided by your PI or their designee
    - (Requires a form submitted to RCR office for final approval and credit)

Visit our website using the QR code above for more information about these workshops and how to register/receive RCR credit for them.

Website: https://research.tamu.edu/research-compliance/responsible-conduct-of-research/workshop-information/

OBJECTIVES

- Provide a general overview of export control regulations
- Discuss export controls in a university setting so you can identify potential concerns
- Provide resources and contacts
- Provide a general overview of the requirements of state's prohibited technology directive
- Discuss ramifications of the state's prohibited technology directive in the university setting
- Provide resources and contacts regarding prohibited technology

EXPORT CONTROLS

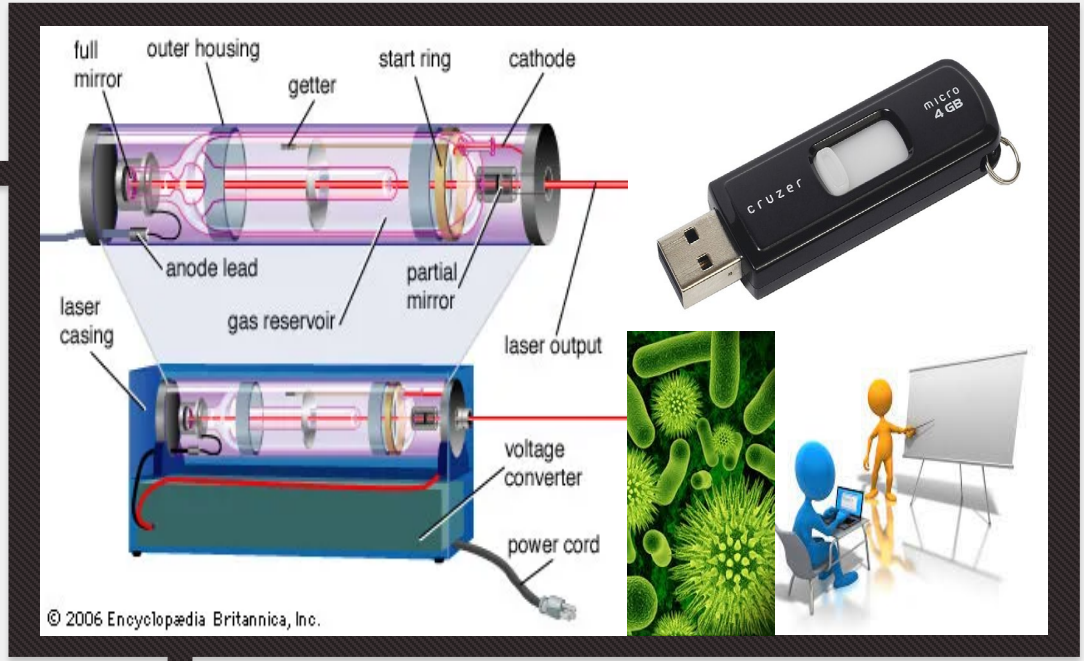
Lauren Douglas
Office of Research Security and Export Controls

WHAT ARE EXPORT CONTROLS?

The term “Export Controls” refers collectively to those U.S. laws and regulations that govern the transfer of controlled information, items or technologies to **foreign countries** and/or **foreign persons**.

The U.S. Government controls certain information, items, technologies, and services deemed to be critical to:

- National Security
  - To prevent terrorism or restrict exports of goods and technology that could contribute to U.S. adversaries’ military potential;
- Economy; and/or
- Foreign Policy.



Penalties for not complying:

- Fines
- Loss of funding
- Bad reputation
- Jail time

WHAT IS AN EXPORT?

WHAT IS AN EXPORT?

- Any item, commodity, technology, or software that is sent out of the U.S. to a foreign destination.
- This includes the physical shipment of goods or items, traveling (or “hand carrying”) controlled items, and electronic or digital transmission of technology or software.

WHAT IS A DEEMED EXPORT?

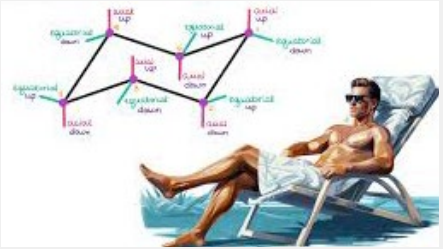
- The transfer of export-controlled information or technologies to a foreign person while IN the United States
- Can involve release of information by:
  - Tours of laboratories & visual inspection
  - Emails
  - Oral conversations

Export Control Regulations apply to BOTH Exports AND Deemed Exports

WHAT IS SUBJECT TO EXPORT CONTROLS?

TANGIBLES

Every tangible item in the U.S. is subject to U.S. export controls, even common everyday items like your computer, chair, pen, etc.



INTANGIBLES

- Specified technology (information) and software **related to controlled items**.

Two Notes:

- U.S.-origin items and technology are still subject to export controls even if they are not currently in the U.S.
- Just because something is available worldwide does NOT mean that US Export Control law don't apply to it.

WHO REGULATES EXPORT CONTROLS?

When discussing export controls, you are going to hear an overwhelming number of acronyms: BIS, EAR, CCL, ECCN, ITAR, USML, OFAC, and SDN (just to name a few).

We’re going to briefly touch on these acronyms: what they stand for, what agencies they belong to, and how they are part of export control regulations on the following slides.

WHO REGULATES EXPORT CONTROLS?

Department of State: Directorate of Defense Trade Controls (DDTC)
International Traffic in Arms Regulations (ITAR)
United States Munitions List (USML)

Department of Commerce: Bureau of Industry and Security (BIS)
Export Administration Regulations (EAR)
Commerce Control List (CCL)

Department of Treasury: Office of Foreign Assets Control (OFAC)
Embargoes and Sanctions on Restricted Entities
Entities listed on the Denied Persons List or Unverified Persons List (among others)

DEPARTMENT OF STATE

Department of State: Directorate of Defense Trade Controls (DDTC)

International Traffic in Arms Regulations (ITAR)

United States Munitions List (USML)

- Covers military items or defense articles
- Controls technologies with inherently military properties
- Regulates goods and technology designed to kill or defend against death in a military setting, as well as defense services (furnishing assistance including design and use of defense articles)
- Includes space related technology because of application to missile technology
- Includes technical data related to defense articles and services
- Typically, you will need to obtain an export license from the U.S. government prior to exporting items, technology, or services covered by the ITAR.
  - Policy of denial for exports to certain countries

DEPARTMENT OF COMMERCE

Department of Commerce: Bureau of Industry and Security (BIS)

Export Administration Regulations (EAR)

Commerce Control List (CCL)

- Regulates items designed for commercial purpose but which could have military applications (computers, civilian aircraft, pathogens)
  - These are known as “Dual Use” controls
- Covers goods, test equipment, materials, biologicals, associated software and technology
- All items specifically named on this list have an Export Controls Classification Number (ECCN)
- Items not listed on the CCL (and not covered by a different regulating body) are still controlled by the EAR, but at the lowest level of control, EAR99.
- If your items is controlled on the CCL, you may need to obtain an export license from the U.S. government prior to exporting it (whether this is a good, software, or technology).

DEPARTMENT OF TREASURY

Department of Treasury: Office of Foreign Assets Control (OFAC)

Embargoes and Sanctions on Restricted Entities

Entities listed on the Denied Persons List or Unverified Persons List (among others)

- Regulates the transfer of items/services of value to embargoed nations
- Imposes trade sanctions, and trade and travel embargoes aimed at controlling terrorism, drug trafficking and other illicit activities
- Economic sanctions focus on end-user or country
- Maintains lists of sanctioned countries and individuals
  - Ex: the SDN – Specially Designated Nationals and Blocked Persons List
- Prohibits payments or providing “value” to nationals of sanctioned countries and certain entities
  - Currently have in place comprehensive embargoes for the following countries: Iran, Syria*, Cuba, North Korea and regions of Ukraine
- If you are trying to do business with (for example ship something to or provide a service to) someone on one of OFAC’s lists, you will need to obtain a license from the U.S. government prior to doing so.
  - Example: You would need a license from OFAC before sending someone in North Korea a coffee cup.

LET'S REVISIT: WHAT IS AN EXPORT?

- An export occurs whenever an item, commodity, technology, or software is sent out of the U.S. to a foreign destination. This includes:
  - Physical shipment of goods or items
  - Traveling with or "hand carrying" controlled items
  - Electronic or digital transmission of technology or software

LET'S REVISIT: WHAT IS A DEEMED EXPORT?

- Release of controlled technology **within the U.S.** to a foreign person
- Deemed Exports are regulated by the same Export Controls as the actual export out of the U.S., and are considered an export to that person's country of residence or citizenship
- NOTE: U.S. citizens or permanent residents ("green card" holders) are NOT foreign persons

CONSEQUENCES OF EXPORT CONTROL VIOLATIONS

- Severe criminal and civil noncompliance penalties and sanctions for **individuals** as well as institutions/corporations
  - Up to $1M for institutions/corporations and up to $500,000 for individuals
  - Up to 20 years in prison
  - Termination of export privileges
  - Suspension and/or debarment from federal government contracting
  - Loss of federal funds

WHAT IS NOT SUBJECT TO EXPORT CONTROLS - EXCLUSIONS?

- **Research** conducted at U.S. universities is often **exempt** from export controls under the following exclusions:
  - Fundamental Research Exclusion
  - Educational Information Exclusion
  - The Public Information Exclusion
- Research results are not subject to U.S. Export Regulations if they fall into one of the above listed exclusion categories.
- Releasing “Technology” or “Software” that arises during or results from, Fundamental Research
- “Technology” is not subject to US export controls if contained in an open (published) patent application.
- “Publicly Available” unclassified Technology or software made available to the public without restrictions through generally available publications including through libraries or other public collections.
- Unlimited distribution at open conference, seminar or trade show.
- Released by instruction in a catalog course or teaching lab.

DEFINITIONS

- Fundamental Research
  - Basic and applied research in science and engineering, the results of which ordinarily are published and shared broadly within the scientific community, as distinguished from proprietary research and from industrial development, design, production, and product utilization, the results of which ordinarily are restricted for proprietary or national security reasons.
- Educational Content
  - Instructional content of curriculum for all students, including foreign nationals, that exist in general science, math, and engineering principles commonly taught through courses and associated teaching laboratories. Must be listed in course catalogs.
- Public Domain
  - Publicly accessible through books, periodicals (hardcopy or electronic) and generally distributed media, unrestricted subscriptions and websites that are free (or available for less than production/distribution costs), libraries, patents or open (published) patent applications, release at open conferences, seminars and trade shows.

EXCLUSIONS

The **Fundamental Research Exclusion** applies to basic and applied research in science and engineering, the results of which are intended to be **published** and shared broadly within the scientific community that has:

- No restrictions on publications
- No restrictions on the participation of foreign nationals
- No specific national security controls on the research or results

Research that meets these conditions is Fundamental Research and the results are NOT subject to U.S Export controls.

The **Education Information Exclusion** applies to information that is **commonly taught** in universities via instruction in catalog courses and/or through the associated teaching laboratories (and is NOT research or design projects).

The **Public Information Exclusion** applies to information that is already published or out **in the public domain**.

Examples include:

- Books, newspapers, pamphlets
- Publicly available technology and software
- Information presented at conferences, meetings or seminars open to the public
- Information included in published U.S. patents
- Websites freely accessible to the public

FUNDAMENTAL RESEARCH EXCLUSION

(IN A LITTLE MORE DETAIL)

FRE can be lost/does not apply if…

- There are restrictions on the publication of the results of the project
  - Pertains to many industry contracts and testing agreements
  - EAR/ITAR do allow for a delay in publication for a pending patent application
- Sponsor approval required prior to publication
  - Sponsor “Review” vs. “Approval”
  - Review period must be temporary
- If participation is limited to US persons or if foreign persons are not permitted

FRE and Deemed Exports…

- Unless the FRE applies, a university’s transfer of controlled technology to a non-permanent resident foreign national may require an export license and/or be prohibited.

Notes:

- **These exclusions only apply to results or information and NOT to physical items**
- FRE may not even apply to all inputs to a project, only the results.

DO EXPORT CONTROLS APPLY TO YOUR RESEARCH?

- Does the research involve military, weapons, defense, chemical or biological weapons, encryption technology & software, space or other dual-use items or export restricted technologies?
- Does the research involve collaboration with any foreign colleagues/collaborators/students either here or abroad?
- Does the research involve the transfer or shipment of equipment, materials or funding out of the U.S.?
- Does any part of the research take place outside of the U.S.?
- Does any part of the research involve the receipt or use of Export Controlled information or items provided by a 3rd party?
- Are there any contractual restrictions on publication or access to or dissemination of the research results?
- Does the research involve any interaction with a sanctioned or embargoed country or with prohibited parties?
- Do you have any reason to believe that the end-user or the intended end-use of the item or information violates any existing export controls?

HOW DO EXPORT CONTROLS APPLY IN A UNIVERSITY SETTING?

- Export controls impact:
  - All international university activities/ interactions (here and abroad).
  - Research projects involving controlled information or technology.

- Examples of University activities where an Export Control review is required:
  - Purchasing equipment or biologicals that are controlled on the USML or CCL
    - Export control (EC) reviews are done on specific commodity coded items in AggieBuy and/or Emburse
  - Traveling overseas on University business (e.g., conferences, conducting field work, international symposia)
    - EC reviews are done on ALL international travel
  - Shipping (or “hand carrying”) anything to a location outside the United States
    - If shipping (or traveling with) something internationally, an EC review should be conducted on the item(s) prior to event
  - Handling controlled information and items
    - EC reviews completed on grants/contracts to identify & set up management plans and appropriate security
  - Any research collaborations with foreign persons and entities
    - EC reviews on disclosures – screening foreign collaborations
  - Visits or tours of research facilities by foreign persons
    - EC reviews may be required before individuals can enter certain labs/areas depending on the research and/or equipment being conducted/housed in the space
  - Providing services or anything of value to an embargoed or sanctioned country
    - EC reviews of vendor set-ups and contracts
  - Grant clauses that potentially prohibit foreign persons or contain publication restrictions
    - EC reviews of grants

EXPORT AUTHORIZATIONS

- When the Export Control Office reviews something (e.g. travel, shipment, foreign collaboration, IRB/IBC/IACUC permit, etc) it is done on a case-by-case basis to answer the questions of WHO, WHAT, WHERE, and for WHAT USE (among others). Each review will generally result in **ONE** of the following outcomes:
  - Not subject to regulations;
  - No license required;
  - License exception (must meet all the requirements);
  - General license (most common for certain activities in embargoed countries); OR
  - Specific License required - requires submission to U.S. Government; this takes additional time and is not guaranteed to be granted

EXPORT AUTHORIZATIONS: SCREENING

End-Use/End User	Embargoes & Sanctions	Restricted or Prohibited Party Lists	High Risk Countries System Regulation 15.05.04 Executive Order GA-48
What is it (e.g. exported item, technology, export-controlled information) being used for? Who is using it? **Potential concerns include:** • Military, nuclear, chemical or biological weapons • Prohibited parties • Plans to divert or transfer to another party	Is it going to a country under a US Embargo or Sanction? • Targeted foreign countries, terrorists, those engaged in activities related to the proliferation of weapons of mass destruction, and other threats. • **Most Restrictive**: Cuba, Iran, North Korea, Russia, Syria, Regions of Ukraine: Crimea, Donetsk, Luhansk • Many other countries with sanctions - each program is specific to the risk in that country	• Lists of parties of concern – if a party to a transaction appears on one of the lists, additional due diligence is required before proceeding. • Depending on the list, a match could indicate strict export prohibition, a specific license requirement, or presence of a "red flag". • Individuals as well as entities can be on the lists. NOTE: This is why we conduct Restricted Party Screening	Effective February 1, 2024, and pursuant to System Regulation 15.05.04, High Risk Global Engagement and High Risk International Collaborations, the following countries and regions are defined as “Countries of Concern” for the current quarter. 1. China; • Hong Kong 2. Cuba; 3. Iran; 4. North Korea; 5. Russia; and 6. Venezuelan politician Nicolás Maduro (Maduro Regime). Effective November 19, 2024, Executive Order GA-48 issued related to hardening state government

RESOURCES

TAMU	TEES	AgriLife
Website: • https://research.tamu.edu/research-compliance/export-controls/ **Contact Information:** • exportcontrols@tamu.edu • 979-862-6419	**Website:** • https://tees.tamu.edu/compliance-operations/research-compliance/export-controls/index.html **Contact Information:** • researchcompliance@tees.tamus.edu	**Website:** • https://agrilifeas.tamu.edu/ethics-compliance/export-controls/ **Contact Information:** • exportcontrols@ag.tamu.edu

Training:

"Export Controls & Embargo Training – Basic Course" via TrainTraq (Course 2111212)

RESPONSIBLE CONDUCT OF RESEARCH CREDIT

To receive RCR credit for today's presentation, please email RCR@tamu.edu with your name, UIN, and notification that you attended this presentation.

Upcoming RCR Sessions:

- **Tuesday, July 1, 2025– 1 hour - Virtual**
  - 10:00-11:00am– RCR – Export Controls
- **Wednesday, July 16, 2025– 1 hour - Virtual**
  - 10:00-11:00am – RCR – Biosafety
- **Thursday, August 21, 2025– 4 hours – In Person (must attend all 4 hours)**
  - 10:00am-2:30pm:
    - Research Data Management
    - Research Security
    - Safe Research Environments
    - Research Misconduct, Authorship & Peer Review
- **Thursday, October 23, 2025– 1 hour - Virtual**
  - 10:00-11:00am – RCR – Animal Welfare
- **The following workshops are available year-round through other departments/offices:**
  - Research Data Management courses – taught through University Libraries
  - Mentor/Mentee courses – taught through the Graduate Mentoring Academy
  - RCR – Lab Specific Training – training provided by your PI or their designee
    - (Requires a form submitted to RCR office for final approval and credit)

Visit our website using the QR code above for more information about these workshops and how to register/receive RCR credit for them.

Website: https://research.tamu.edu/research-compliance/responsible-conduct-of-research/workshop-information/

PROHIBITED TECHNOLOGY

PROHIBITED TECHNOLOGY

WHAT IS IT? A QUICK OVERVIEW…

- Basically, a ban on certain technologies that include:
  - Specific hardware and software
- Originated from a Governor's directive regarding Tiktok
- Over time, expanded to include other things (hardware and software from specific companies)
- Generally, without an approved exception, we cannot purchase, install, or use those prohibited technologies
- As a public university of the state of Texas, we must comply the governor's directive and State laws
- Where you may have questions about a specific technology, communicate with your local IT personnel

PROHIBITED TECHNOLOGY BACKGROUND

TIMELINE

- **December 7, 2022:** Governor Greg Abbott issued a directive requiring all state agencies to ban TikTok from state-owned devices and networks due to national security concerns over potential surveillance capabilities.
- **February 6, 2023:** Governor announces statewide model security plan for state agencies to address vulnerabilities presented in the use of TikTok and other software on personal and state-issued devices.
- **June 14, 2023:** Texas Legislature passed Senate Bill 1893 adding Texas Government Code Chapter 620, which legally prohibits covered applications on governmental entity devices.

PROHIBITED TECHNOLOGY BACKGROUND

TIMELINE

- **July 12, 2023:** Texas A&M University System issues systemwide security plan; directs members to implement "*administrative, operational, or technical security controls*" as necessary to comply.
- **October 7, 2024:** The Texas A&M University System's Covered Applications and Prohibited Technology Plan memorandum directing system members to, among other things, implement any necessary administrative, operational, or technical security controls to prohibit the use or download of covered applications and prohibited technology on all member-owned devices.
- **January 31, 2025:** Governor issued a ban prohibiting the use of artificial intelligence (AI) and social media apps affiliated with the People's Republic of China (PRC) and the Chinese Communist Party's (CCP) on government-issued devices.
- **April 8, 2025:** TAMUS Regulation 29.01.06 "Covered Applications and Prohibited Technologies" approved.

TAMUS REGULATION 29.01.06 “COVERED APPLICATIONS AND PROHIBITED TECHNOLOGIES”

29.01.06 **Covered Applications and Prohibited Technologies**

Approved April 8, 2025
Next Scheduled Review: April 8, 2030

Regulation Summary

This regulation implements Texas Government Code Chapter 620 and the Governor’s Directive to State Agency Heads, December 7, 2022 (Governor’s Directive”), in respect to protecting the state of Texas from software, applications, hardware, and equipment that pose a risk to the state of Texas if the developer or manufacturer may be required by a foreign government, or an entity associated with the foreign government, to provide confidential or private personal information collected by the software, application, hardware, or equipment to the foreign government or associated entity without substantial due process rights or similar legal protections; or the software, application, hardware, or equipment poses a similar risk to the state’s sensitive information and critical infrastructure. Chapter 620 of the Texas Government Code and Governor’s Directive require The Texas A&M University System (system) to remove covered applications and prohibited technologies published on the DIR Covered Applications and Prohibited Technologies list from state-owned and state-issued devices, and to block access to prohibited technologies from state-owned networks. This regulation applies to the system and its members, including their employees, contractors, interns, and any users of member-owned networks.

WHAT ARE THE PROHIBITED TECHNOLOGIES?

CERTAIN SOFTWARE/APPLICATIONS/DEVELOPERS

- Alipay
- ByteDance Ltd.
- CamScanner
- DeepSeek
- Kaspersky
- **Lemon8**
- Moomoo
- QQ Wallet
- **RedNote**
- SHAREit
- Tencent Holdings Ltd.
- Tiger Brokers
- **TikTok**
- VMate
- WeBull
- WeChat
- WeChat Pay
- WPS Office
- *Any subsidiary or affiliate of an entity listed here.*

WHAT ARE THE PROHIBITED TECHNOLOGIES?

CERTAIN HARDWARE/EQUIPMENT/MANUFACTURERS

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

WHAT ARE THE PROHIBITED TECHNOLOGIES?

COVERED APPLICATIONS

- Lemon8
- RedNote
- *TikTok or any successor application or service developed or provided by ByteDance Ltd. or an entity owned by ByteDance Ltd.*

COVERED APPLICATIONS AND PROHIBITED TECHNOLOGIES

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

- **Covered applications** are limited to certain social media applications and services, such as TikTok. The prohibition against covered applications extends beyond institution-owned devices, and exceptions are extremely limited to law enforcement and information security purposes.
- **Prohibited technologies** are a broad set of hardware and software products and services specified by the Texas Department of Information Resources (DIR). The prohibition has a broad set of technical and administrative requirements that **apply to both institution-owned devices and personally-owned devices used for state business.**

SUBSIDIARIES OR AFFILIATES

REGARDING "SUBSIDIARY OR AFFILIATE"

- Only the TAMU System Office of General Counsel can determine whether a particular technology qualifies as a "subsidiary or affiliate" for the purposes of this regulation. Contact the IT Risk Management office (it-security@tamu.edu) with any questions, or for clarification about specific technologies.

TAMUS SAP 29.01.06 “COVERED APPLICATIONS AND PROHIBITED TECHNOLOGIES”

1

Prevent TikTok and prohibited tech on state devices and networks

Includes all state-issued devices capable of internet connectivity

2

Prohibit state business on prohibited tech-enabled personal devices

Personal devices only allowed if managed by the agency

3

Identify sensitive locations

Includes virtual meeting rooms — personal devices NOT allowed in

4

Exception Process

Limited exceptions that must be approved by the university president

IMPACT ON UNIVERSITY OPERATIONS

University-owned Devices

- Employees who use only institution-owned, Technology Service-managed devices, software, and other technologies to do their job should experience little to no impact.
- If you currently use a prohibited technology for state business, discontinue the use of the prohibited technology and contact your IT Risk Management (it-security@tamu.edu) for further guidance.
- Prevent the use or download of any prohibited tech on all university-owned devices
  - Includes desktops, laptops, tablets, cell phones, other internet-capable devices
  - Centrally manage university-owned devices to monitor compliance; maintain ability to remotely wipe devices and uninstall prohibited software
- Prevent communication with prohibited applications on all university networks or devices
  - Manage networks with firewall rules and VPN configurations
  - Manage devices using endpoint management tools

IMPACT ON UNIVERSITY OPERATIONS

PERSONALLY-OWNED DEVICES

- **Prohibit employees or contractors from using personal devices with prohibited technology to conduct university business**
- **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 state business. If you are required to conduct state 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.
- Within the scope of this prohibition, using your personal device as part of Duo/Microsoft/etc. Multi-Factor Authentication (MFA) is not considered conducting state business.

IMPACT ON UNIVERSITY OPERATIONS

Personally-owned Devices

- Prohibit personal devices with prohibited hardware from connecting to technology infrastructure
  - Applies specifically to local (TAMU) networks
  - Connections to public-facing technology (such as a public website) are excluded

IMPACT ON UNIVERSITY OPERATIONS

Sensitive Areas

- Identify, catalog, and label locations designated as **sensitive areas**
  - Generally, information owners designate a sensitive area
  - Sensitive areas are defined as any location, physical or logical (virtual meetings), that are used to discuss or create research product that is considered Confidential or Internal Use information **of a sensitive nature that must be protected** from unauthorized disclosure or public release.
- Identify and catalog data that requires protection of sensitive areas
- **Prohibit** employees or contractors from bringing personal **devices with prohibited tech into designated sensitive areas**
  - Visitors are subject to this policy

IMPACT ON UNIVERSITY OPERATIONS

PROCUREMENT CONTROLS

- Prevent procurement of any hardware or software that meets the criteria published by DIR
  - AggieBuy looks for certain key words
- What is the operational definition of subsidiary or affiliate?
  - *DIR has not defined this*
- No positive responsibility to search for corporate structure information
  - Once notified of a subsidiary or affiliate relationship, the university must act
- If in doubt regarding if a device or software is considered prohibited technology, communicate with your local IT personnel- we will assist if needed.

IMPACT ON UNIVERSITY OPERATIONS

SUMMARY

- Institution-owned devices cannot have prohibited technologies installed or access covered applications.
- Personal devices used for state business cannot have prohibited technologies installed if used for conducting university work (e.g. accessing your university email).
- University networks may block access to prohibited technologies and restrict devices with these technologies.
- Purchasing decisions must consider whether hardware or software appears on the prohibited list.

OTHER PRECAUTIONS

- Periodically review the Texas DIR Covered Applications and Prohibited Technologies web page (https://dir.texas.gov/information-security/covered-applications-and-prohibited-technologies) as it is periodically updated.
- If a student or grad student is procuring hardware or software for a project or research, ensure they too are aware of the prohibited technologies criteria.
  - This includes purchases made personally, as they cannot be reimbursed.
- *It is possible that a technology not prohibited today could be acquired by a prohibited technology vendor in the future, and as a result render that previously not prohibited technology prohibited.*

EXCEPTION PROCESS

Exception Process Summary

Limited exceptions may be available for some prohibited technologies (*but not for covered applications such as TikTok*):

- Contact the Office of the CISO (ciso@tamu.edu) to request an exception
- Provide detailed business justification for the technology
- Exceptions require approval from the university president
- Exceptions are limited to one year
- No exceptions are permitted for covered applications under TGC Chapter 620

EXCEPTION PROCESS

- **Limited exceptions** may be granted for some prohibited technologies
- Exceptions may **only** be approved by the agency head (university president)
  - Exceptions are only valid for one year and must be renewed annually
- All approved exceptions must be reported to Texas DIR through the TAMU CISO
- Devices granted an exception should only be used for the specific use case and only on non-state or specifically designated separate networks
  - If possible, cameras and microphones should be disabled on those devices when not in active use for their intended purpose
- There is a further-limited exception process for covered applications, such as Tiktok (e.g. restricted to law enforcement or public safety investigations)

EXCEPTION PROCESS

- **Information about research is required where an exception is requested**, such as:
  - **Project description** and whether research is funded or unfunded.
  - **Justification of prohibited tech-** Why is the use of this technology imperative to the research?
  - **What other comparative technologies were reviewed?**
  - **Why are other comparative technologies insufficient?** *Describe in detail.*
- **An approved technology and data management plan** is required, specifying:
  - The use of the technology as part of the overall project.
  - The risk mitigation measures that will be in place.
  - Plan must be approved by the Office of the TAMU CISO.
- **Notifications** will be sent to:
  - Your Dean, Department Head, and/or Vice President (for administrative units)
  - Vice President for Research and Responsible Conduct in Research Office
- Ultimate approval must be granted by the university president (state rule)
- Texas DIR will be notified; **exceptions are for 1 year**

RESOURCES

- The Texas A&M University System's Covered Applications and Prohibited Technology Plan: https://it.tamu.edu/policy/it-policy/laws-regulations/TAMUS%20Prohibited%20Technologies%20Plan%20Memo%20October%202024.pdf
- TAMU Laws and Regulations page: https://it.tamu.edu/policy/it-policy/laws-regulations/index.php
- TAMUS SAP 29.01.06 "Covered Applications and Prohibited Technologies": https://policies.tamus.edu/29-01-06.pdf
- TAMUS Prohibited Technology page: https://www.cyber.tamus.edu/policy/guidelines/prohibited-technology/
- TAMUS Prohibited Technology FAQs page: https://www.cyber.tamus.edu/policy/guidelines/prohibited-technology/faq/

RESOURCES

- Governor's Order Against Tiktok: https://gov.texas.gov/news/post/governor-abbott-orders-aggressive-action-against-tiktok
- Statewide Model Security Plan: https://gov.texas.gov/uploads/files/press/Statewide_Plan_for_Preventing_Use_of_Prohibited_Technology_in_State_Agencies_(Final_OOG).pdf
- State Bill 1893: https://capitol.texas.gov/tlodocs/88R/billtext/pdf/SB01893I.pdf
- Texas Government Code 620: https://statutes.capitol.texas.gov/Docs/GV/pdf/GV.620.pdf
- **Texas DIR Covered Applications and Prohibited Technologies** page: https://dir.texas.gov/information-security/covered-applications-and-prohibited-technologies
- GA-48: https://gov.texas.gov/uploads/files/press/EO-GA-48_Hardening_State_Government_FINAL_11-19-2024.pdf

RESOURCES

Contact Information

- For questions regarding prohibited technology, send an email to it-security@tamu.edu

THANK YOU