TTU IT Resources

IT Help Center Advanced Computing Services, contact (903) 742-4357 (HELP) or advcomputing@ttu.edu.

Jennifer Horn, J.D.
Faculty, staff, and students at Texas Tech will likely, at one time or another, interact with federal regulations that impose access, dissemination, or participation restrictions on the transfer of information created or maintained by federal departments and agencies. These regulations are intended to protect the national security, foreign policy, anti-terrorism or non-proliferation of critical technologies.

Texas Tech’s Cybersecurity Practices

Backdoors, unauthorized access or use of computing devices, or unauthorized copying, disclosure, dissemination, or retention of information can result in prosecution for Federal laws and regulations.

In case you require assistance, please contact Jennifer Horn, J.D. for assistance before proceeding:

You are planning to disclose, ship, transmit, or transfer any item, information, or software that has been designed, developed, configured, adapted, or modified for military or intelligence applications.

You plan to export any tangible items or goods to another country, including one of the countries with restrictions; embargo; or any item, information, or software that is subject to any defense-embargo.

You are providing a “service of value” to an individual or organization located in a foreign country, including nations that are subject to embargoes or trade sanctions.

You are providing a service to the military or intelligence agencies.

You are providing a service to a foreign government or military.

Texas Tech’s Cybersecurity Practices

In some cases, researchers may require a higher level of encryption technology and assistance with encryption solutions. In those situations, the Texas Tech community is dealing with US export control regulations. The Texas Tech Operating Policy for foreign export control (SP 74.12) establishes policies for federal laws and regulations governing the export of information, products, and technology. If you find yourself in any of the following situations as an employee of Texas Tech, please contact Jennifer Horn, J.D. for assistance before proceeding:

For more information about HPCC services, equipment, or grid computing at TTU, please visit our website http://www.hpc.ttu.edu, email hpc@ttu.edu or call (806) 742-4350.

Data Safety While Traveling Abroad

Adapted from FIS Counter Intelligence Divestment Program

American academic freedom and the advanced research & development (R&D) conducted at Academic Institutions have resulted in progress in innumerable fields of research. As a result of these advancements, the US export control regulations have become stricter. In these cases, the IT Division can work directly with the researchers to develop a customized solution. For assistance with a customized solution for highly sensitive research data, please contact the TTU IT Security Team at security@ttu.edu or (806) 742-0840.

Research Data and Information Activity

The TTU IT Division collaborates with the Vice President for Research, Office of Research to provide guidelines regarding researchers engaged in international travel and research travel. Office of Responsible Research, as well as the Chief Information Officer, can provide guidance, based on your particular circumstance.

Data Encryption

University policies that require sensitive or confidential data is stored or copied to mobile devices, such as laptops, then the data must be encrypted. The IT Division provides a whole disk encryption solution from Symantec, formerly PGP Corporation, that will satisfy the encryption requirements for most users, including researchers. For information and assistance with encryption using PGP, please contact IT Help Center at (806) 742-4357 (HELP) or email at ithelp@ttu.edu.

In some cases, researchers may require a higher level of encryption technology for certain types of data. In these cases, the IT Division can work directly with the researchers to develop a customized solution. For assistance with a customized solution for highly sensitive research data, please contact the TTU IT Security Team at security@ttu.edu or (806) 742-0840.

Export Control

Jennifer Horn, J.D.

Faculty, staff, and students at Texas Tech will likely, at one time or another, interact with federal regulations that impose access, dissemination, or participation restrictions on the transfer of information created or maintained by federal departments and agencies. These regulations are intended to protect the national security, foreign policy, anti-terrorism or non-proliferation of critical technologies.

Texas Tech’s Cybersecurity Practices

In some cases, researchers may require a higher level of encryption technology and assistance with encryption solutions. In those situations, the Texas Tech community is dealing with US export control regulations. The Texas Tech Operating Policy for foreign export control (SP 74.12) establishes policies for federal laws and regulations governing the export of information, products, and technology. If you find yourself in any of the following situations as an employee of Texas Tech, please contact Jennifer Horn, J.D. for assistance before proceeding:

You are planning to disclose, ship, transmit, or transfer any item, information, or software that has been designed, developed, configured, adapted, or modified for military or intelligence applications.

You plan to export any tangible items or goods to another country, including one of the countries with restrictions; embargo; or any item, information, or software that is subject to any defense-embargo.

You are providing a service to the military or intelligence agencies.

You are providing a service to a foreign government or military.

Texas Tech’s Cybersecurity Practices

In some cases, researchers may require a higher level of encryption technology for certain types of data. In these cases, the IT Division can work directly with the researchers to develop a customized solution. For assistance with a customized solution for highly sensitive research data, please contact the TTU IT Security Team at security@ttu.edu or (806) 742-0840.

Research Data and Information Activity

The TTU IT Division collaborates with the Vice President for Research, Office of Responsible Research to provide guidelines regarding researchers engaged in international travel and research travel. Office of Responsible Research, as well as the Chief Information Officer, can provide guidance, based on your particular circumstance.

Data Encryption

University policies that require sensitive or confidential data is stored or copied to mobile devices, such as laptops, then the data must be encrypted. The IT Division provides a whole disk encryption solution from Symantec, formerly PGP Corporation, that will satisfy the encryption requirements for most users, including researchers. For information and assistance with encryption using PGP, please contact IT Help Center at (806) 742-4357 (HELP) or email at ithelp@ttu.edu.

In some cases, researchers may require a higher level of encryption technology for certain types of data. In these cases, the IT Division can work directly with the researchers to develop a customized solution. For assistance with a customized solution for highly sensitive research data, please contact the TTU IT Security Team at security@ttu.edu or (806) 742-0840.
Workstations – Desktop and Laptop Computers connected to TTUnet

• Install Symantec Endpoint Protection for Windows and Mac OS workstations available on the University site during the semester (https://eraider.ttu.edu). You can also purchase a CD from the ATLC available via the University site license free of charge through the eRaider website (http://eraider.ttu.edu). You can also purchase an installation CD from the ATLC available via the University site license free of charge through the eRaider website (http://eraider.ttu.edu). You can also purchase an installation CD from the ATLC available via the University site license free of charge through the eRaider website (http://eraider.ttu.edu).

• Configure and maintain Windows and Mac OS workstations.

Update and patch Windows Operating System (OS)

• Use automatic critical updates. Instructions are available at http://askit.ttu.edu/updates.

• Use Microsoft Update to manually install on a regular basis.

• Update and patch Unix/Linux Operating System (OS)

Linux distributions include utilities for automatically applying updates such as yum, apt-get, and up2date. Note that while you enable these utilities, your computer may need to be set up with automatic, schedulable updates like yum, apt-get, and up2date, to reduce the risk of not receiving important patches at any time.

Mobile Devices

• Always use a PIN/Password that locks your device automatically when not in use.

• Use automatic locks after 2 minutes.

• Ensure that Google Play and Apple App Stores are restricted to prevent individuals from installing and running applications that could negatively impact custom applications.

• Update your directories for security purposes.

• Use secure protocols when accessing and communicating confidential and sensitive information.

• Using encryption technologies is also recommended.

• Eliminate data from devices that you transfer to TU Surplus Property with secure data deletion tools or software.

• Utilize the University storage resources such as OneDrive for Business and Microsoft Office 365 OneDrive to backup data and retrieve data from previous versions.

• Keep multiple backups of research data in secure, off-site locations.

Data Classification

• Define Confidential and Sensitive Data

• Confidential Data is defined by the Texas Administrative Code Chapter 185.001 which aims to protect information against accidental or unauthorized disclosure.

• Public or sensitive public data is based on rules of specific federal or state law.

• The University (nuuu.edu) has procedures in place to protect personal or personally identifiable information and also to protect classified or sensitive information.

• Data Classification policies and procedures are available to students and staff.

• Access Control data, Account Management data, procedures, security policies, and access to resources, or any other ITU data owners must designate.

• Data Classification

• Research data should be classified with regard to its confidentiality and access control requirements. Data may take precedence over public release based on state or federal law or other legal agreement.

• The TTU Security Policies (www.depts.ttu.edu) are available for public release based on state or federal law or other legal agreement.

• Personal Health Information (PHI)

• PHI for all researchers and students.

• The IT Division created Red RaiderPC (www.redraiderpc.ttu.edu) to provide affordable shredding service on campus. Clean out your old file deletion tools or software; and

•Using encryption technologies is also recommended.

• Eliminate data from devices that you transfer to TU Surplus Property with secure data deletion tools or software.

• Utilize the University storage resources such as OneDrive for Business and Microsoft Office 365 OneDrive to backup data and retrieve data from previous versions.

• Keep multiple backups of research data in secure, off-site locations.

• Without the appropriate departmental access credentials, only individuals with a "need-to-know" can access system directory files physically or remotely; and

• Best practice in the use of encryption

Data Backup and Storage Options

• The University offers a central data backup service for computers within the TTU Community. For assistance using eRaider to manage access to confidential or sensitive data – TTU’s Office365 OneDrive – personal version instead of enterprise version (OneDrive for Business). For assistance at (806) 742-4357 (HELP) or email ithelpcentral@ttu.edu

• The TTU IT Division and the Operations Division are partnering to provide an affordable shredding service on campus. Clean out your old file deletion tools or software; and

• The IT Division created Red RaiderPC (www.redraiderpc.ttu.edu) to provide an affordable shredding service on campus. Clean out your old file deletion tools or software; and

• For assistance using eRaider to manage access to confidential or sensitive data – TTU’s Office365 OneDrive – personal version instead of enterprise version (OneDrive for Business). For assistance at (806) 742-4357 (HELP) or email ithelpcentral@ttu.edu

• Donating departments should return equipment per TTU’s IT Security Team

• Sensitive Data - Information pertaining to Restricted, Research, Security, or Public Release Based on State or Federal Law or Other Legal Agreement.

• Data Classification

• Research data should be classified with regard to its confidentiality and access control requirements. Data may take precedence over public release based on state or federal law or other legal agreement.

• The TTU Security Policies (www.depts.ttu.edu) are available for public release based on state or federal law or other legal agreement.

• Personal Health Information (PHI)

• PHI for all researchers and students.

• The IT Division created Red RaiderPC (www.redraiderpc.ttu.edu) to provide an affordable shredding service on campus. Clean out your old file deletion tools or software; and

• Using encryption technologies is also recommended.

• Eliminate data from devices that you transfer to TU Surplus Property with secure data deletion tools or software.

• Utilize the University storage resources such as OneDrive for Business and Microsoft Office 365 OneDrive to backup data and retrieve data from previous versions.

• Keep multiple backups of research data in secure, off-site locations.

• Data Backup and Storage Options

• The University offers a central data backup service for computers within the TTU Community. For assistance using eRaider to manage access to confidential or sensitive data – TTU’s Office365 OneDrive – personal version instead of enterprise version (OneDrive for Business). For assistance at (806) 742-4357 (HELP) or email ithelpcentral@ttu.edu

• The TTU IT Division and the Operations Division are partnering to provide an affordable shredding service on campus. Clean out your old file deletion tools or software; and

• The IT Division created Red RaiderPC (www.redraiderpc.ttu.edu) to provide an affordable shredding service on campus. Clean out your old file deletion tools or software; and

• Donating departments should return equipment per TTU’s IT Security Team

• Sensitive Data - Information pertaining to Restricted, Research, Security, or Public Release Based on State or Federal Law or Other Legal Agreement.

• Data Classification

• Research data should be classified with regard to its confidentiality and access control requirements. Data may take precedence over public release based on state or federal law or other legal agreement.

• The TTU Security Policies (www.depts.ttu.edu) are available for public release based on state or federal law or other legal agreement.

• Personal Health Information (PHI)

• PHI for all researchers and students.

• The IT Division created Red RaiderPC (www.redraiderpc.ttu.edu) to provide an affordable shredding service on campus. Clean out your old file deletion tools or software; and

• Using encryption technologies is also recommended.

• Eliminate data from devices that you transfer to TU Surplus Property with secure data deletion tools or software.

• Utilize the University storage resources such as OneDrive for Business and Microsoft Office 365 OneDrive to backup data and retrieve data from previous versions.

• Keep multiple backups of research data in secure, off-site locations.

Embedded Operating Systems in Research Equipment

Some research equipment has an internal computing system that includes an operating system. If you need to connect to the TTU network, contact the TTU Security Team (806) 742-8040 or askit.ttu.edu

Cybersecurity Resources

Review detailed guidelines for data access, and applications at the TTU Cybersecurity Practices Website (http://cybersecurity.ttu.edu)