    - 52.02 Infringement of Copyrights in Information Technology (IT)
    - 52.03 Obtaining Telecommunication Services
    - 52.04 Information Technology (IT) Security
    - 52.05 Electronic and Information Resources Accessibility
    - 52.06 Project Management Practices
    - 52.07 Website Operations
- TTU IT Security Policies http://it.ttu.edu/security

TTU High Performance Computing Center

The High Performance Computing Center (HPCC) provides consulting and assistance to campus researchers with experimental software and/or hardware needs, training in parallel and grid computing, and administration for local high performance systems.

High performance computing resources available:

- Hrothgar – A heterogeneous cluster of 12-core Westmere nodes and 20-core Ivy-Bridge nodes for a total of 9,456 cores over 724 nodes. The Center uses a mixture of DDR IB (20 GigE) and QDR IB (40 GigE) for low latency, high bandwidth nodes running parallel jobs, and standard 1GigE for nodes running serial jobs. There is a shared 1.6 PB file system;
- Community Cluster – A collection of compute and storage nodes purchased and used by various research groups. There are currently 182 nodes and 1 PB of storage;
- Janus – A Window's HPC cluster with 12 20-core Ivy-Bridge nodes each with 64GB of RAM and 1GigE bandwidth;
- TechGrid – Campus-wide grid of 2,000 3.0 GHZ Dell PCs with 24 Teraflops of peak performance, leveraging unused compute cycles; and
- Lonestar – HPC Cluster located at UT Austin which we have the equivalent of 1,940 cores.

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

Data Encryption

University policies require that if sensitive or confidential data is stored on 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 Central at (806) 742-4357 (HELP) or email at ithelpcentral@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.

Research Data and International Activity

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

Export Control

Jennifer Horn, J.D.

Faculty, staff, and students at Texas Tech will likely, at one time or another, intersect with federal regulations that impose access, dissemination, or participation restrictions on the transfer of items and information regulated for reasons of national security, foreign policy, anti-terrorism or non-proliferation. In these situations, the Texas Tech community is dealing with US export control regulations. The Texas Tech Operating Policy for Export Control (OP 74.10) 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 travel or send items, information, or software to Cuba, Iran, North Korea, Sudan, Syria, or other countries subject to sanctions or an embargo;
- You are providing a "service of value" to an individual or organization located in one of the countries with restrictions;
- You plan to export any tangible items or goods to another country, including any university-owned equipment that is being hand-carried on travel;
- You plan to disclose, ship, transmit, or transfer any technology or software that is not "publicly available;"
- You are planning to disclose, ship, transmit, or transfer any item, information, or software that will be used to support military training of any foreign units or forces, regular or irregular;
- You are planning to disclose, ship, transmit, or transfer any "defense article," or any item, information, or software that has been designed, developed, configured, adapted, or modified for military or intelligence applications;
- You intend to engage in activities that have the potential to relate to proliferation of nuclear explosive devices, chemical, or biological weapons, missile technology and/or the proliferation of chemical weapons; and/or
- You are or plan to be involved in a transaction with a person/organization that is a "party of concern." See http://www.export.gov/ecr/egmain_023148.asp

Data Safety While Traveling Abroad

Adapted from FBI Counter Intelligence Domain Program

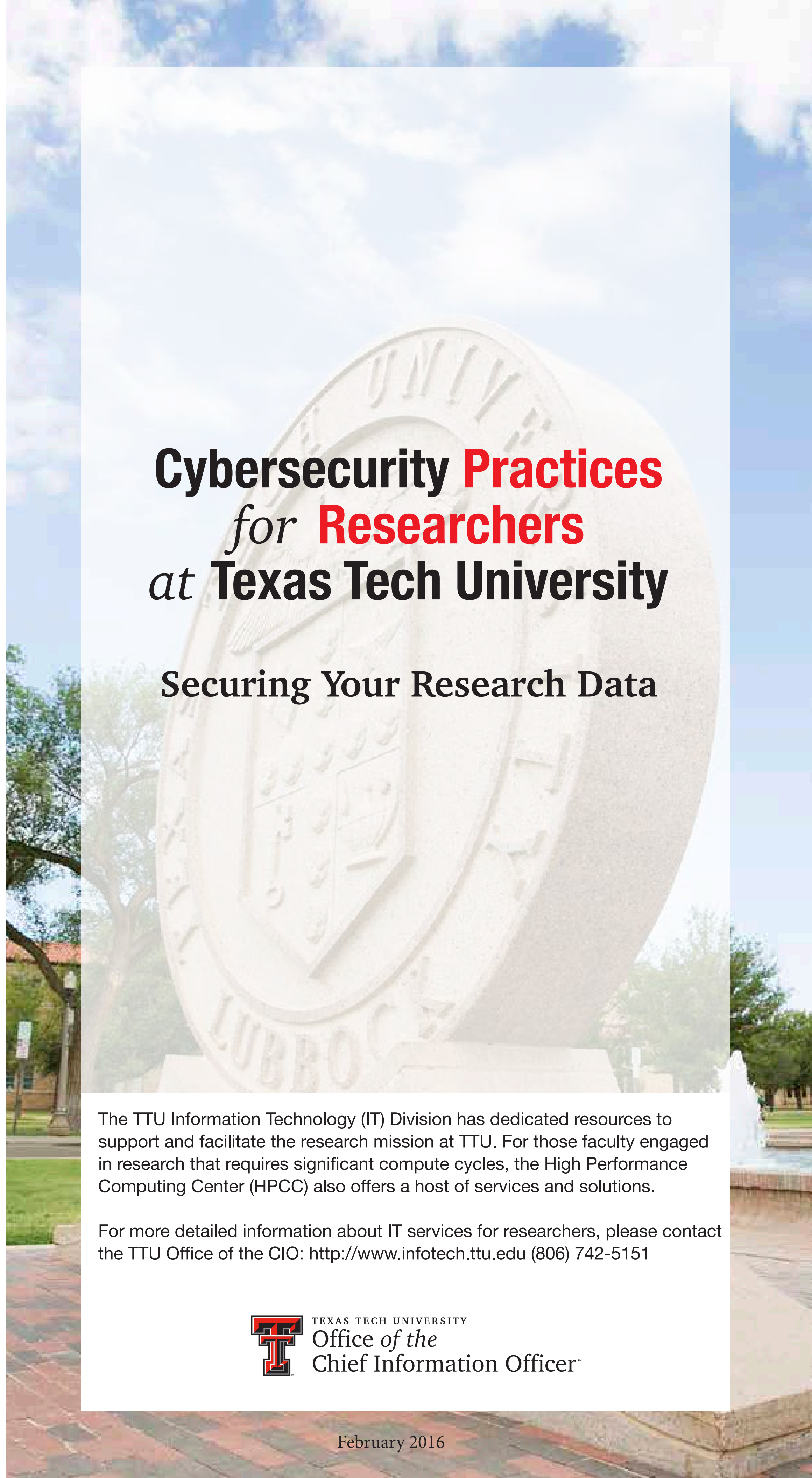
American academic freedom and the advanced research & development (R&D) conducted at Academic Institutions have resulted in progress in innumerable areas. But, there are still some considerations to help protect your students and your R&D from being stolen by other researchers, or used by hostile foreign governments and/or their military agencies:

- Prior to your travel, be sure to visit http://travel.state.gov/content/travel/english.html or https://www.cia.gov/library/publications/the-world-factbook/index.html to obtain country background, updated travel advisories, and the current political situation of the countries being visited;
- Do not travel with any unnecessary information or current research on a laptop;
- Avoid placing internet addresses ("favorites") on any laptop you take. Take only that info which you will present or discuss at the conference;
- Do not leave your laptop unattended;
- Make sure your laptop is password protected;
- Do not continue to use a laptop that begins to run slowly, or acts strangely after taking it overseas. Have the system professionally analyzed for viruses or spyware before and after travel. Recognize that your personal belongings may be searched several times; and
- Be aware of unsolicited requests sent to you on the Internet, persons asking questions about your research, and persons requesting your opinion as to the status of others' research being conducted at the Academic Institution. Information about failures in research can be as valuable as successes. Be careful in discussing any research that is not your own.

TTU IT Resources

- IT Help Central Advanced Computing Services, contact (806) 742-4357 (HELP) or advcomputing@ttu.edu.
- Site-Licensed Software available for TTU Faculty; for more information contact Technology Support at (806) 742-1650 or it4researchers.ttu.edu.

Software List	Cost for TTU Researchers
Adobe Creative Cloud	None (faculty/staff only)
AutoCAD	None
CBT - (SkillSoft)	None, cbt.ttu.edu
ESRI	None
JAWS	$602/license
JMP	None
LabView	None (faculty/staff only)
Maplesoft	$10/per CD
Matlab	None
Microsoft Office 365	None, office.com
REDCap	None, evaluate.ttu.edu
SAS	$120/license/Fiscal Year
SPSS	$100 new; $80 renewal/license/Fiscal Year
Symantec Antivirus	None
Visual Studio Standard	None, Dream Spark
Window Upgrades	Upgrades for TTU campus machines only



Cybersecurity Practices *for* Researchers *at* Texas Tech University

Securing Your Research Data

The TTU Information Technology (IT) Division has dedicated resources to support and facilitate the research mission at TTU. For those faculty engaged in research that requires significant compute cycles, the High Performance Computing Center (HPCC) also offers a host of services and solutions.

For more detailed information about IT services for researchers, please contact the TTU Office of the CIO: http://www.infotech.ttu.edu (806) 742-5151

TEXAS TECH UNIVERSITY
Office *of the*
Chief Information Officer

February 2016

Workstations – Desktop and Laptop Computers connected to TTUnet

- Install Symantec Endpoint Protection for Windows and Mac OS workstations, 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 Reception Desk, located in the west basement of the main Library building;
- Configure and maintain firewall settings;
- Update and patch Windows Operating System (OS)
  - Enable automatic critical updates; instructions are available at http:// askit.ttu.edu/winupdate.
  - Use Microsoft Windows Update to manually install on a regular basis.
- Update and patch Unix/Linux Operating System (OS)
  - Linux distributions have utilities for automatically applying updates such as yum, apt-get, and up2date. Note that when you enable these utilities, you will need to disable automatic updates, as the required restart may negatively impact custom applications.
  - Consult your distribution's technical support for those custom applications prior to upgrading your UNIX OS.
- Add systems to the TTU.EDU domain; for more information visit https://www.askit.ttu.edu and search for "TTU.EDU domain" and your operating system. For additional information on protecting your workstation, refer to the Workstation Hardening policy at http://www.depts.ttu.edu/infotech/security/docs/workstation_hardening.php.

System Authentication and Security

Make sure that only authorized individuals with a business "need-to-know", have access to confidential and sensitive data. TTU IT can assist you with access control using eRaider, or you may choose to designate access within an application using local accounts. Please consult with your departmental IT staff, or you may contact TTU IT Help Central to locate an IT Division professional who can assist you. We recommend the following practices:

- Use eRaider authentication for access to computer systems, applications, and databases, whenever feasible. For assistance using eRaider to manage access control, please contact IT Help Central;
- Use strong passwords. (Password integrity relies heavily upon the password length, complexity, reuse, and aging). Our eRaider Account Management System enforces strong password policies, but you should use this same approach for any other accounts;
- Do not use your eRaider password for any other accounts;
- Change default administrator account passwords;
- Enhance the security of data stored on your hard drive by restricting those who can access system directory files physically or remotely; and
- Lock workstations when you are away from your system, and use auto locking after two minutes of inactivity.

Desktop-level Access to Data

- TTU Windows desktops and workstations must be joined to the TTU domain in order to ensure logins utilize eRaider, and that minimum security settings are in place;
- 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 TTU Surplus Property with secure file deletion tools or software;
- Utilize the University storage resources such as OneDrive for Business and TechShare to store mission critical data; and
- Keep multiple backup copies of research data in secure, off-site locations.

Mobile Devices

- Always use a PIN/Password that locks your device automatically when not in use;
- Use auto locks after 2 minutes;
- Ensure your mobile device uses native encryption – typically native encryption is enabled by default or enabled when you set a PIN/Password lock;
- Do not disable the security settings on your mobile device, and check your settings periodically as Internet criminals use malicious apps to disable security settings ("jail broken" device), leaving the device and your data unsecured;
- Do not use unapproved cloud-based storage services such as Dropbox™, GoogleDocs, or OneDrive* for TTU confidential or sensitive data – TTU's Office365 OneDrive for Business is approved for limited types of confidential or sensitive data – for assistance, email itcompliance@ttu.edu;
- Avoid downloading and installing apps and games that could compromise your device or expose your personal information – only download apps from official app stores/sites known to be reputable; and
- For more information about mobile device security and connectivity to TTU networks, visit http://askit.ttu.edu and enter the search terms "mobile device security" or "mobile device connectivity."

*OneDrive - personal version instead of enterprise version (OneDrive for Business)

Server Security

- Join all production servers to the TTU domain (TTU.EDU); contact IT Help Central for assistance at (806) 742-4357 (HELP) or email ithelpcentral@ttu.edu;
- House your server(s) in a secure, climate-controlled environment; the University Data Center (managed by TOSM) provides hosting services; contact (806) 742-2900 or email serversupport.tosm@ttu.edu for additional information and services;
- Refer to the Server Hardening IT Security Policy for specific configuration practices at http://it.ttu.edu/security/docs/server_hardening.php;
- Register your server and coordinate with the TTU IT Security Team; contact security@ttu.edu or (806) 742-0840. The security team routinely conducts vulnerability scanning and reporting;
- Be aware that some grants and sponsored research projects may have additional security requirements, and the TTU IT Division is equipped to assist you with these additional requirements, including Department of Defense mandates, as we have DOD security cleared personnel;
- Create a disaster recovery plan for your data and applications; and
- Routinely review security logs daily and report any suspicious activity to the TTU IT Security Team at security@ttu.edu. For your protection, please contact the security team immediately before you attempt to remediate or investigate the problem, as you may inadvertently destroy pertinent evidence and information.

Data Collection and Management

- Defining Confidential and Sensitive Data
  - Confidential Data is defined by the Texas Administrative Code Chapter 202 as "information that must be protected from unauthorized disclosure or public release based on state or federal law or other legal agreement." Texas Tech University OP 70.40 details procedures and safeguards regarding private or personally identifiable information; and
  - Sensitive Data - Information pertaining to Restricted, Research, Access Control data, Account Management data, procedures, security documentation of Information Resources, or any other information TTU data owners so designate.
- Data Classification
  Research data should be classified with regard to its confidentiality and criticality. To protect research data, researchers must take measures to protect access, secure storage, and prevent data loss, based on the type (classification) of data involved. The TTU IT Security Policies (www.depts.ttu.edu/infotech/security/) define data types and associated requirements.
- Personal Health Information (PHI)
  For areas with potential use of PHI, TTU and TTUHSC have made arrangements to accomodate and secure this data. Please contact the TTU Information Security Officer at security@ttu.edu to request assistance.

Data Disposal

- The IT Division created RaiderPCMart (http://www.raiderpcmart.ttu.edu) to facilitate the exchange of computers and peripherals within the TTU Community, allowing departments to recycle computers that are still usable;
- Donating departments should clean the hard drive of any exchanged equipment using a secure data erasure program so that data cannot be retrieved by the new owner. To ensure that all data is permanently erased from a hard drive, use a program such as the KillDisk utility, available free at http://www.killdisk.com/downloadfree.htm. KillDisk rewrites every "bit" of information on hard drives or other media several times, making recovery of any data extremely difficult. For assistance in removing the content from your system with KillDisk, please contact your NSC or IT Help Central 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 cabinets and closets and call Red Raider Shred, (806) 742-8327 (TEAR), to schedule a pickup. Your old documents will be shredded and recycled. For more information including TTU document retention policy information, please see www.depts.ttu.edu/services/redraidershred/Shred_Week.php;
- Secure file deletion and free space wiping tools for Linux
  - Wipe:
    http://sourceforge.net/projects/wipe
  - Scrub:
    http://sourceforge.net/projects/diskscrub
  - DBAN:
    http://sourceforge.net/projects/dban/
- All hard drives from TTU surplus computers are removed and shredded before those systems leave the University. Individual hard drives can also be shredded upon request by contacting Red Raider Shred at (806) 742-8327 (TEAR). Red Raider Shred can provide a certificate of destruction that conforms to NIST 800-88, upon request.

Data Backup and Storage Options

- The University offers a central data backup service for computers within the TTU domain with mission critical data; for more information visit https://www.askit.ttu.edu, and search "for data backup and storage options"; and
- Data Storage: Store research data on a secure TTU system. As the TTU IT Division works to continuously enhance data security practices at TTU, we encourage the University community to take advantage of data storage options available centrally, including:
  - OneDrive (for individuals) and TechShare (for departments). Both storage areas are backed-up nightly and housed in a secure and stable environment;
  - SharePoint sites can be created upon request for use by TTU Colleges and Departments. SharePoint sites enable secure document storage, management, and collaboration;
  - Microsoft Office 365 OneDrive for Business is a cloud-based storage service available to TTU faculty, staff, and students. OneDrive for Business provides storage, collaboration, and file/folder synchronization between computers, tablets, and smartphones;
  - TTU Research Data Repository – Beginning Spring 2016, the IT Division in collaboration with the University Library and Office of the VPR will provide a new Research Data Repository for TTU researchers. This repository will provide secure online storage for both active and archived research data. Researchers interested in utilizing this new service should contact the High Performance Computing Center (HPCC) at (806) 742-4350 or at hpcc@ttu.edu; and
  - For information regarding these and other centrally available storage services, please contact IT Help Central at (806) 742-4357 (HELP) or email ithelpcentral@ttu.edu.

Protection of Research Labs

- Secure physical access to research labs. Contact the TTU Police Department for consultation on ways to protect physical access to research labs;
- Conduct a criminal background check on employees handling research data; and
- Consult with TTU Environmental Health and Safety to guard against environmental hazards, and to comply with hazardous chemicals and associated data. For more information contact the Office of the Vice President for Research at (806) 742-3905 or email techvpr@ttu.edu.

Embedded Operating Systems in Research Equipment

Some research equipment has an internal computing system that includes an operating system. If you need to connect equipment to the TTU network, contact the TTU IT Security Team at security@ttu.edu or (806) 742-0840.

Cybersecurity Resources

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

- IT Operating Policies http://www.depts.ttu.edu/opmanual/contents.php#52
  - 52.01 Information Technology (IT) Operations