Protecting TTU Information Resources

Cybersecurity landscape refers to the combination of cyber threats, security strategy, available technology solutions, and the current status of security at any given time. To facilitate uninterrupted and effective teaching, learning, and research activities at TTU in this environment, our IT staff work in partnership with executive leadership, administrators, faculty, and staff in key areas such as Procurement Services, Contracting, and General Counsel. Most importantly, we work with the many Network Site Coordinators (NSCs – our departmental IT contacts) who partner with us to secure and protect institutional information resources, while assisting faculty, staff, and students.

Securing data is specific to the network infrastructure and to the types of data and demographics present at Texas Tech. Security controls span from the basic anti-malware tools and training to advanced Artificial Intelligence (AI) and machine-language based network firewalls and security software to fend off phishing attacks, ransomware, Denial-of-Service attacks, and hacker intrusion attempts. Information at Texas Tech is protected based on the Federal NIST C-I-A (Confidentiality – Integrity – Availability) triad framework. The IT OPs, especially OP 52.01 and OP 52.04, are designed to protect institutional information resources and are aligned with Texas Administrative Code (TAC) §202 and by extension, the Federal NIST SP 800-53 cybersecurity framework, as required by the State of Texas.

As mandated by TAC, these security programs and practices are reviewed biennially by an independent assessor, selected from a pre-approved list of security vendors provided by the Texas Department of Information Resources. Additionally, there are newer more stringent requirements by the Federal government to protect federal research data in accordance with the NIST 800-171 framework. The Cybersecurity training and awareness program at Texas Tech is also compliant with the requirements mandated by HB 3834 from the 86th Legislative Session, 2019. To enhance information security at Texas Tech University, significant investments have been made over the last few years, including the increase in IT security staff and training, hardening of network infrastructure and critical systems, providing secure data storage, multi-factor authentication, and use of enhanced security tools.

One of the key methods in securing university information resources is with judicial use of limited budget resources is via pre-approved IT solutions (most of them with input from the campus community), including the creation of major institutional contracts, such as Microsoft, Blackboard, Dell, and Apple, with appropriate educational discounts for both institutional and research use by faculty, staff, and students. Due to security concerns, some systems, such as Huawei, ZTE, Lenovo, and Lexmark systems, are not approved for use at Texas Tech University for institutional use.

There are many policies and procedures in place to protect institutional information resources, but, ultimately, the campus community plays a significant role in helping in these efforts, by adhering to established policies, becoming more self-aware of cybercrime (information is available at http://cybersecurity.ttu.edu), and by protecting institutional information under their control (see OP 70.40).

Thank you for helping to protect our institutional information resources. If you have questions, please contact IT Help Central at (806) 742-4357 (HELP) or via email at ithelpcentral@ttu.edu.
For many years, Skype for Business (SfB), integrated with the Texas Tech University email system, has served as our institution’s primary phone and communications tool. Microsoft is in the process of transitioning from SfB to Teams. Texas Tech is currently in this transition phase where both SfB and Teams are being used. Both tools offer unique features and functionality. Here are some recommendations on which tools are best for various situations:

**Skype for Business**
- Telephone functions
- Inbound, outbound, direct dial employee phone calls
- Departmental phone calls, including receptionist functions
- Location information for 911 emergency responders
- Presence – Automated availability information based on SfB activity and calendar information, or manual selection
- Integration with Microsoft Office apps, University-provided cloud storage (SharePoint Online, OneDrive), and other third-party apps, including chat function
- Online meetings up to 50 attendees (with telephone dial-in and dial-out options)

**Microsoft Teams**
- Best tool for ongoing team and project collaborations
- Presence – Automated availability information based on Teams activity and calendar information, or manual selection
- Integration with Microsoft Office apps, University-provided cloud storage (SharePoint Online, OneDrive), and other third-party apps, including chat function
- Online meetings up to 300 attendees (meeting dial-in and dial-out options upon request)
- Webinars up to 10,000 attendees at no charge
- Synchronous course delivery for classroom instruction, as well as asynchronous communication and collaboration beyond the classroom
- Class teams that provide special capabilities tailored for teaching and learning
- Full session recording and transcription

**TTU Migrates to Top Hat for Learning Engagement Tool**

Over the next couple of years, Texas Tech will continue migrating functionality from SfB to Teams to align with Microsoft’s product support schedule for SfB, which will end in 2025. Our transition will include the migration of telephone and location functions. Some equipment replacement may be necessary over the next couple of years to take full advantage of Teams functionality. TTUHSC and TTUHSC El Paso have technology initiatives to upgrade their own phone and communications tools so that they can connect with our Teams environment.

During this transition, Texas Tech University and Texas Tech University System Administration employees should continue to sign in to SfB for telephone functionality and location information for 911 calls, and also Teams for collaboration functions and meetings. **After the migration, SfB will be discontinued, and Teams will provide all the functionality currently provided by Teams and SfB.**

In addition to SfB and Teams, we also provide a couple of other communication and collaboration tools to enrich the teaching and work experience at the University:

**Zoom Conferencing**
- Synchronous classroom instruction and online meetings up to 300 attendees (with dial-in options)
- Webinars up to 10,000 attendees (additional charge to departments for larger webinars and/or dedicated webinar licenses)
- Full session transcription

**Blackboard Collaborate Ultra**
- Synchronous classroom instruction up to 250 attendees (with dial-in options)
- Live virtual sessions with students
- Native integration with the TTU Learning Management System, Blackboard Learn

For more information, questions, or assistance, please contact IT Help Central at (806) 742-4357 (HELP) or ithelpcentral@ttu.edu.

The timing of Top Hat implementation has proven to be beneficial as we strive for more interactive pedagogies, particularly as we consider strategies that minimize physical contact, yet allow for immediate student feedback. Top Hat has robust solutions that leverage student devices and meet their accommodation needs.

We recognize that transitioning to a new instructional technology requires time and energy that may seem in short supply. To assist in this process, the Office of the Provost has funded resources to help faculty migrate their materials to the Top Hat solution. If you are interested in these services or have any questions, please feel free to reach out to Dr. Kathy Austin (kathy.austine@ttu.edu), Dr. Justin Louder (justin.louder@ttu.edu), or Suzanne Tapp (suzanne.tapp@ttu.edu). The IT Division has also developed a site regarding Texas Tech’s engagement with Top Hat.

Over the Summer of 2022, we have removed other engagement tools from our Blackboard environment, and have worked collaboratively with campus responseware users to migrate them to the Top Hat platform.
As children continue to increase the amount of time spent on the internet, they also increase their chances of encountering online predators. Hiding behind the anonymity of the computer screen allows these predators to gain your child’s trust more easily, and in turn, leaves your child vulnerable to exploitation. It is extremely important for parents and guardians to take an active role in their children’s activities and create an environment of trust in which children feel comfortable discussing who they are communicating with through websites and apps, what activities they are participating in online, and the safety precautions they are taking.

Enough Is Enough, one of the nation’s leading internet safety organizations, created Internet Safety 101, a digitally-based internet safety resource designed to educate, equip and empower parents, educators and other adults with the knowledge and resources they need to protect children from internet dangers.

The series encourages parents to watch for warning signs of contact with an online predator, such as:

- Becoming secretive about online activities;
- Getting angry when he or she cannot get online;
- Withdrawing from family and friends; or
- Changing screens or turning off computer when an adult enters a room.

Some suggested tips for online safety are listed below:

- Know your children’s online account information - screen names, passwords, etc., and ensure their profiles are set to “private”;
- Pay attention to what your kids are doing online and ask your child non-threatening questions, such as:
  - Has an online stranger...
    - Asked you for personal information?
    - Said anything to make you feel uncomfortable?
    - Asked you for pictures?
- Check regularly that any photos/videos they post do not contain any personally identifiable information or reveal where you and your child live;
- Remind your children that the people they meet online may be lying about their identity so never meet with or call someone they do not know in real life; and
- Remind your children to think before they post: there are no take-backs online.

Additional information on navigating social media can be found at https://internetsafety101.org/parentsguidetosocialmedia or cybersecurity.ttu.edu.

Reminder: Keep Your eRaider Password Secure

Do not enter your eRaider password on a website unless you are certain it is a Texas Tech website. Hackers are very skilled at creating web pages that look identical to TTU web pages. You can find tips for identifying fraudulent websites at https://www.askit.ttu.edu/IDfraudsite.

Familiarize yourself with TTU’s password policy and tips for creating a secure password.

We encourage you to be vigilant in practicing cybersecurity and invite you to learn more at cybersecurity.ttu.edu. For more information, assistance, or if you have questions, please contact IT Help Central at (806) 742-4357 (HELP) or via email at ithelpcentral@ttu.edu.

~ Parents’ Corner ~

Online Predators