Message from the CIO

As many conduct various spring cleaning efforts, we remind you to include organizing and “cleaning up” your digital assets as a part of that activity. Spring cleaning presents an ideal opportunity for the TTU community to minimize digital clutter and securely dispose of paper records containing confidential or sensitive institutional information that are no longer needed (See OP 10.10: Records Retention). To assist with this task, we provide information on storage management and optimizing shared University resources. Our Spring Cleaning Bulletin also offers guidance on maintaining a clean computer in the challenging West Texas climate, as well as cleaning and sanitizing mobile devices. Also included is a reminder to review your social media presence as part of your digital spring cleaning. Finally, to help ensure that our digital assets are in order, we provide information about proper licensing for all software installed on University-owned devices. As a quick reminder, Microsoft announced a critical vulnerability in Outlook, so be sure to update your devices, if you have not already. Go Tech!

—Sam Segran, Vice President for IT and Chief Information Officer

Storage Management: Optimize University Resources

In the spirit of “digital cleaning,” the TTU IT Division encourages you to schedule time to sort through your institutional files and emails. Reviewing your email inbox, folders, and archives will help you stay organized and conserve institutional data storage resources.

We recommend the following practices when storing and managing electronic files:

- Establish a system to organize the files you send, receive, and store;
- Delete old/unwanted files you are not required to retain (Records Retention OP 10.10);
- Be sure to check any Deleted Items, Sent Items, or Junk folders regularly; and
- Archive old files that you need to retain (records retention schedule).

Additionally, the IT Division provides the following resources to faculty and staff at no charge, such as:

- **Blackboard**—learning management system;
- **Mediasite**—enterprise lecture capture system;
- **OneDrive for Business**—online storage for individuals;
- **SharePoint Online**—storage for departments, groups, projects, etc.; and
- **Microsoft Teams**—multi-purpose communications platform used for education and business at TTU.

To view an expanded list of educational and enterprise IT services, please visit [https://www.askIT.ttu.edu](https://www.askIT.ttu.edu), and click on “IT Services.”

Thank you in advance for your partnership in the strategic management of institutional resources.

For detailed instructions and support, please contact IT Help Central at (806) 742-4357 (HELP) or [ithelpcentral@ttu.edu](mailto:ithelpcentral@ttu.edu).
The Challenge of West Texas Dust: Maintaining a Clean Computer in the West Texas Climate

General Cleaning Tips
- Clean your device immediately if it comes into contact with any damage-causing material (liquid, oils, sand, etc.);
- Do not spray cleaners directly onto the device;
- Unplug all external power sources, devices, and cables when cleaning the device;
- You may use 70% isopropyl alcohol, disinfecting wipes, or a similar product without bleach;
- Avoid getting any moisture into device crevices, and consider using a small crevice brush to clean out debris;
- Do not use aerosol sprays, bleaches, ammonia, or abrasives;
- Use only a soft, lint-free cloth. Do not use paper towels, tissues, or similar because they are abrasive; and
- Avoid excessive wiping, which might cause damage.

In addition to regular cleaning, the TTU IT Division also suggests the following environmental practices:
- Keep the area surrounding your computer clean and free from obstructions that would prevent proper airflow; avoid stacking papers or other items on or near your computer. Clutter and stacked items can act as insulation and retain heat, taxing the PC’s internal cooling mechanism.
- Keep liquids away from the PC, keyboard, mouse, printer, and other peripherals.
- Keep magnetic devices away from the PC, as they can cause severe damage to the PC and its components.

Microsoft Announced a Critical Vulnerability in Microsoft Outlook

As TTU IT announced in mid-March, a serious vulnerability has been discovered in Windows desktop versions of Outlook. This vulnerability can be exploited if you receive or open a malicious email. If successfully exploited, an attacker could gain access to sensitive information, including passwords, and potentially launch attacks on other services and devices.

Microsoft quickly corrected this vulnerability in a March Microsoft Office 365 update, that would have already automatically installed on your system, if Office Automatic Updates were enabled. If you do not have Office Automated Updates, we recommend that you do so, and we provide instructions at www.askIT.ttu.edu. The TTU IT Division recommends updating your installations, including personal systems, as soon as possible to keep your information safe! If you maintain systems for faculty, staff, computer labs, and classrooms, please verify that the installations are updated on those systems.

As a reminder, the following cybersecurity practices can help protect your information and TTU data and information resources:
- Do not click on links or open attachments contained within an email unless you are certain of the sender's identity and expecting the information;
- Delete and do not reply to any suspicious emails;
- Update your desktop, laptop, and/or mobile device anti-virus software;
- Do not download and install applications from unknown or untrusted sources; and
- Keep current on critical system updates:
  - Windows: https://askit.ttu.edu/windowsupdate
  - macOS: https://askit.ttu.edu/macupdate
  - iOS and iPadOS: https://askit.ttu.edu/iosupdate
  - Android: https://askit.ttu.edu/androidupdate

We encourage you to be vigilant in practicing cybersecurity and invite you to learn more at: http://cybersecurity.ttu.edu. For more information or questions, please contact IT Help Central at (806) 742-4357 (HELP) or via email at ithelpcentral@ttu.edu.
Digital Cleaning: Remember Your Social Media

Be sure to add social media to your digital cleaning checklist. While Facebook, Instagram, Snapchat, Twitter, YouTube, and Slack are heavily used across generations for recreation and entertainment, these platforms may store personal and sensitive information.

For example, many social media users disclose a plethora of personal information about family, friends, ancestry, and current demographics. In addition to reviewing your personal information online, we also recommend following these three suggestions to “clean up” your social media accounts:

**Review and remove old posts or photos.**
Where possible, look through old posts, comments, and photos. Remove photos and posts that contain personally identifiable information for you and your family. Social networking sites are notorious repositories of personally identifiable information that cybercriminals can use against us!

Information like “mother’s maiden name,” “model of your first vehicle,” “name of your high school,” or “name of your first pet” are all common security questions associated with email, bank accounts, and much more!

**Scan your friends and followers lists.**
Look through your friends and followers lists, and remove accounts of people you may not know, may not wish to stay connected with, or suspect might be fake accounts.

If you receive a friend request from someone that is already on your friend list, be cautious about accepting the request as their account may have been compromised.

**Update your privacy settings.**
Now that you have done most of your “clean up,” look at your privacy settings. Make sure you are in control of who can view your profile information, as well as who can tag you in various posts, comments, or photos. Review the level of access to your information that you have granted to friends, friends of friends, or the public.

Consider restricting your posts to people that you know “in the real world.” Check your privacy settings every few months, as they may change.

---

**Removal of Unauthorized Software on University-Owned Devices**

As part of our digital spring clean-up, Texas Tech University reminds all employees, students, departments, and units about the importance of proper software licensing. Most software packages require acceptance of an End User License Agreement (EULA) at the time of installation. However, TTU employees and students, as well as departments and units, do not have the authority to sign any EULA on behalf of the university, per Operating Policy and Procedure 72.09 and Regents’ Rules Chapter 07.12.

Additionally, “Personal,” “Free,” “Consumer,” and “Trial” software packages often forbid installation on organization-owned systems, including those owned by Texas Tech University, without a legitimately acquired software license. Software license purchases and all related contract documents are approved and authorized by Procurement Services and the TTU Office of the CIO. Any software package, installed on a University-owned device, that is not properly licensed through the TTU System, University, or your department is a violation of copyright laws and TTU policies, and must be removed immediately. Some software packages are licensed at the Texas Tech University System level (i.e., Oracle, Ellucian) for software shared among Texas Tech institutions; others are licensed at the institutional (TTU) level (i.e., Microsoft 365, Adobe), and some may have been licensed by a department for a few systems or users in their area. For anti-malware, please only use Microsoft Defender for Endpoint for both TTU-owned Windows and macOS systems.

We ask that you review software installed on area/department institutionally-owned systems and ensure that all software is properly licensed, typically through a TTU software site license or an area/department purchase.

**For further information, please contact:**
- University Data Center at serversupport@ttu.edu for assistance with institutional virtual servers;
- Technology Support Licensing at itts.licensing@ttu.edu for questions about software licensed for campus use;
- Procurement Services at purchasing@ttu.edu for information about the procurement and contract process for any license; or
- IT Help Central at ithelpcentral@ttu.edu or (806) 742-4357 (HELP) for general IT assistance, including questions about software and hardware.

Remember, proper software licensing is not only essential for legal compliance, but also for ensuring the security and reliability of TTU’s digital infrastructure. Let’s all work together to keep our systems safe and properly licensed.

View IT Bulletins online at infotech.ttu.edu/itbulletin

Computer-Based Training (CBT): cbt.ttu.edu