Department of Environmental Toxicology
College of Arts and Sciences
Texas Tech University

1207 GILBERT DRIVE * LUBBOCK, TX 79416 * 806-885-4567 (tel) * 806-885-2132 (fax)

Computing Policies / Procedures

Effective Date: June 30, 2018

Author: _____
Lori Gibler, Assistant Director Information Technology Date

Chairperson: _____
Steve Presley, Ph.D. Date

Contents

PURPOSE

The Department of Environmental Toxicology (ENTX) Domain represents a communication resource, for both educational and research missions, whose very design requires shared and cooperative use. The primary purpose of this document is to record the policies, procedures, and accepted conventions of use that govern use and management of the Department of Environmental Toxicology (ENTX) computing and networking resources.

REVIEW

The ENTX Information Technology Administrator, will review this ENTX document on an annual basis and after any incident.

Drills or exercises must be conducted at least annually to test and evaluate the effectiveness of the computing operating policies and procedures. The computing operating policies and procedures must be reviewed and revised, as necessary, after any drill or exercise and after any incident.

The Quality Assurance/Safety Manager will act as The ENTX Quality Assurance/Safety Manager Administrator.

POLICY/PROCEDURE

1. Acceptable Use Policy

1.1. General Use and Ownership

1.1.1. ENTX proprietary information stored on electronic and computing devices remains the sole property of the ENTX. ENTX employees must ensure that proprietary information is protected.

1.1.2. ENTX employees have the responsibility to report the theft, loss or unauthorized disclosure of ENTX proprietary information.

1.1.3. ENTX employees may access, use or share ENTX proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.

1.1.4. ENTX employees will not be allowed to use ENTX computers and equipment for personal use.

1.1.5. ENTX employees must not use software listed in the "Unauthorized Software Policy".

1.1.6. ENTX employees must not degrade the performance of ENTX computers and equipment; deprive an authorized user access to ENTX computers and equipment; obtain extra computers and equipment beyond what is allocated; and/or circumvent computer security measures.

1.1.7. The ENTX Information Technology Administrator reserves the right to audit the network and computing systems on a periodic basis to ensure compliance with this policy.

1.2. Security and Proprietary Information

1.2.1. All mobile and computing devices that connect to the TTU network must comply with the University Computing Policies and the Policies and Procedures outlined in this document.

1.2.2. System level and user level passwords must comply with the "Password Policy". Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

1.2.3. All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less.

1.2.4. ENTX employees must report any vulnerabilities in computer security or any incidents of possible misuse to ENTX Information Technology Administrator.

1.2.5. ENTX employees must not share their accounts, passwords, Personal Identification Numbers (PIN), or devices used for identification and authorization purposes. ENTX employees who share their access with another individual shall be responsible and held liable for all usage of their account.

1.2.6. ENTX employees must not download, install or run security programs or utilities that reveal or exploit vulnerabilities in the security of ENTX computers and equipment.

1.3. Unacceptable Use

1.3.1. Accessing data, a server or an account for any other purpose other than conducting ENTX business, even if you have authorized access, is prohibited.

1.3.2. Introduction of malicious programs into the ENTX network or server (e.g., viruses, worms, Trojan horses, etc.).

1.3.3. Revealing your account password to others or allowing use of your account by others.

1.3.4. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not

an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

1.3.5. Port scanning or security scanning is expressly prohibited.

1.3.6. Executing any form of network monitoring which will intercept data intended for the ENTX server and client computers.

1.3.7. Circumventing user authentication of security of any ENTX computer, network or account.

1.3.8. Using any program/script/command with the intent to interfere with, or disable, any ENTX computer.

1.3.9. Providing information about ENTX computing and network to individuals outside the ENTX.

2. Antivirus / Antispyware Protection Policy

2.1. All ENTX computers/servers have controls in place that is designed to prevent malicious code (e.g., computer viruses, worms, and spyware) from compromising the confidentiality, integrity, or availability of information systems.

2.2. ENTX computers/servers use Symantec Endpoint Protection with the following features:

2.2.1. Antivirus and Antispyware Protection to protect against viruses, Trojan horses, and spyware.

2.2.2. Proactive Threat Protection to provide zero-day protection against unknown threats.

2.2.3. Network Threat Protection to provide against network threats.

2.3. ENTX computers/servers us Malwarebytes Anti-Malware with the following features:

2.3.1. The scanner supports multiple drive scanning including network drives with the option to perform a quick scan, full scan, or flash scan. The flash scan will analyze memory and auto run objects.

2.3.2. The protection module automatically quarantines file system threats and blocks malicious code.

2.4. Always scan floppy diskettes/CDs/DVDs/thumb drives from an unknown source for viruses before using it.

2.5. Backup critical data to the ENTX server on a regular basis.

2.6. If lab testing conflicts with antivirus software, run the antivirus software to ensure a clean computer, disable the antivirus software, then run the lab tests. After the lab test, enable the antivirus software. When the antivirus software is disabled, do not use floppy diskettes/CDs/DVDs/thumb drives that could transfer a virus.

3. Bluetooth Device Policy

3.1. No Bluetooth device shall be deployed on ENTX equipment that does not meet a minimum of Bluetooth v2.1 specifications without written authorization for the ENTX Information Technology Administrator.

3.2. When pairing the Bluetooth device to Bluetooth enabled equipment (i.e. phone, laptop, etc.), ensure that you are not in a public area where your PIN can be compromised.

3.2.1. If your Bluetooth enabled equipment asks for you to enter your PIN after you have initially paired it, you must refuse the pairing request and report it to the ENTX Information Technology Administrator.

3.3. Activate Bluetooth only when it is needed.
3.4. Bluetooth mode must be turned off when not in use.
3.5. Personal Identifiable Information and/or ENTX confidential or sensitive data must not be transmitted or stored on Bluetooth device hardware, software or connections.
3.6. Bluetooth device hardware, software or connections that do not meet the standards of this policy shall not be authorized for deployment.
3.7. Bluetooth users must act appropriately to protect information, network access, passwords, cryptographic keys, and Bluetooth equipment.
3.8. Bluetooth users are required to report any misuse, loss, or theft of Bluetooth devices or systems immediately to the ENTX Information Technology Administrator.
3.9. Eavesdropping, device ID spoofing, DoS attacks, or any form of attacking other Bluetooth enabled devices is unauthorized.
3.10. Using ENTX owned Bluetooth equipment on non-ENTX owned Bluetooth enabled devices is unauthorized.
3.11. Modification of ENTX owned Bluetooth devices for any purpose is unauthorized.

4. Computer Inventory Policy

4.1. The ENTX Quality Assurance/Safety Manager is responsible for maintaining the inventory of ENTX's computing assets. To insure the accuracy of ENTX's computing inventory, all computing hardware and software purchases will be approved by the ENTX Information Technology Administrator and coordinated through ENTX purchasing agent.
4.2. When faculty, staff or students leave ENTX, the ENTX Information Technology Administrator and the ENTX Quality Assurance/Safety Manager will take possession of all computing devices listed in section 8.3.7. The ENTX Information Technology Administrator will redistribute the computing equipment to areas of greatest need.
4.3. The ENTX Information Technology Administrator will receive, install, and configure all new computing hardware and software.
4.4. If inventory tagged ENTX computing equipment needs to be moved, the ENTX Information Technology Administrator and the ENTX Quality Assurance/Safety Manager must be informed prior to the move in order to update the inventory records as to the new location of the tagged equipment.
4.5. If inventory tagged ENTX computing equipment needs to be salvaged, the ENTX Information Technology Administrator and the ENTX Quality Assurance/Safety Manager must be informed prior to salvage pickup in order to fill out the proper paperwork and update the inventory records.
4.6. If inventory tagged ENTX computing equipment needs to be removed from ENTX property to an employee's personal residence, a research location, or other like property to accomplish ENTX work, a Temporary Use of Equipment Authorization form must be completed and signed. This form is available through ENTX Quality Assurance/Safety Manager.

5. Computer Purchases Policy

5.1. The ENTX Information Technology Administrator is responsible for all computing hardware and software purchases.
5.2. Funding for computing purchases will be as follows:
5.2.1. Faculty computers will be provided by the Faculty representative funds.

5.2.2. Staff computers will be purchased via the ENTX director's office funds.
5.2.3. Graduate student computers will be provided by the Faculty representative funds.

6. Copyright Policy

6.1. Federal copyright laws protect most software available for use on ENTX computers. Educational institutions are not exempt from the laws covering copyrights.
6.2. The software provided through the ENTX for use by faculty, staff, and students may be used only on computing equipment as specified in the various software licenses.
6.3. It is the policy of ENTX to respect the copyright protections given to software owners by federal law.
6.4. It is against ENTX policy for faculty, staff, or students to copy or reproduce any licensed software on ENTX computing equipment, except as expressly permitted by the software license.
6.5. Faculty, staff, and students may not use unauthorized copies of software on ENTX computers.
6.6. Unauthorized use of copyrighted materials (including software, graphic images, music or audio files, and written word) is regarded as a serious matter and is a violation of the ENTX policy, the University policy, and federal law.
6.7. The owner of the copyrighted material may expose any individual who reproduces copyrighted material to both the ENTX and University disciplinary action and possible legal action.

7. Computer Updates Policy

7.1. All ENTX computers are configured for regular patching and updates made to operating systems and individual applications.
7.2. Windows updates are configured to check for updates every day. Important updates are installed automatically.
7.3. All users are given permission to install windows updates on their workstation computer.
7.4. The ENTX Information Technology Administrator will install windows updates on the ENTX servers and lab computers.
7.5. Recommended updates are downloaded to the computer but not installed until the user initiates the installation.
7.6. Windows update provides updates for Microsoft products, Microsoft software, and computer hardware.

8. Electronic Data Policy

8.1. Electronic data security is the responsibility of both the ENTX Information Technology Administrator and ENTX personnel to protect against natural disasters, computer espionage, computer system failures, data corruption, or system operation errors. Data protection includes all computer-related activities capable of receiving, storing, managing, or otherwise transmitting electronic data.
8.2. Software
8.2.1. ENTX personnel may not install software on ENTX computing devices operated without the approval of the ENTX Information Technology Administrator.
8.2.2. Lab software requests must be approved by the Lab Director and the ENTX Information Technology Administrator.

8.2.3. The ENTX Information Technology Administrator will install and maintain the software.

8.3. Hardware, peripheral devices and data storage devices

8.3.1. Protection of ENTX hardware, peripheral devices and data storage devices are the responsibility of both the ENTX Information Technology Administrator and ENTX personnel.

8.3.2. Passwords may not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.

8.3.3. Whiteboards containing restricted and/or sensitive information must be erased.

8.3.4. Computer workstations must be locked when workspace is unoccupied.

8.3.5. Computer workstations must be locked or shut completely down at the end of the work day.

8.3.6. Laptops, Hard Drives or Portable peripheral devices must never be unattended.

8.3.7. Examples of hardware, peripheral devices and data storage include, but are not limited to, the following:

- Desktops / Laptops
- Internal / External Hard Drives
- Monitors
- Tablet devices
- USB flash / Thumb drives
- USB patch cords with mini / micro connectors
- Electronic notebooks
- Smartphones
- PDA’s
- CD-R/DVD-R’s
- Memory cards
- Future technological development

9. **Electronic Data Protection Policy**

9.1. ENTX personnel are responsible for the protection of electronic data not stored on ENTX servers.

9.2. Examples of electronic data include, but are not limited to, the following:

- online display of information
- downloaded information
- computer printouts
- storage media
- transmissions

9.3. ENTX personnel are responsible for managing their personal use of electronic data; including but not limited to, password security and use of their TTU accounts.

9.4. ENTX personnel are accountable for their actions and any activity resulting from a breach in password security on their TTU accounts.

9.5. ENTX personnel are responsible for the immediate reporting of suspected or confirmed violations to the ENTX Information Technology.

10.**Email Policy**

10.1. Email (TechMail) is provided by the Texas Tech University and is the official means of communication within the University system.
10.2. ENTX personnel are responsible to maintain and check their TechMail account regularly.
10.3. ENTX personnel are accountable to know information disseminated through their TechMail account.
10.4. Failure to read University and/or Departmental TechMail account communications sent to ENTX personnel does not absolve them from knowing and complying with the content of these communications.
10.5. If an individual is separated from ENTX for questionable, dishonest, or dubious behavior, email accounts will be terminated immediately.

11.**Network Domain Policy**

11.1. The Network Domain within the ENTX is designed, installed, maintained and operated by TTUnet.
11.2. TTUnet will diagnose all physical problems with the network.
11.3. Attachment of Ethernet repeaters, bridges, routers, switches, hubs, or any other network device by anyone but TTUnet is prohibited because attachment of such equipment is a violation of the ENTX and University network security policies.
11.4. Unauthorized modifications to the TTU network are not allowed. If you feel modifications are needed, you MUST contact ENTX Information Technology Administrator.
11.5. Any modification to the TTU network without prior approval from the ENTX Information Technology Administrator violates Network and Computing Security Policy.

12.**Network and Computing Security Policy**

12.1. The ENTX Information Technology Administrator may terminate or restrict an individual network connection without notice in the event that the ENTX Information Technology Administrator judges that the individual network connection presents an immediate security risk to the ENTX equipment, software, or data.
12.2. Any security violation of the ENTX resources will be brought to the attention of the appropriate authorities as outlined in the TTU Computing Security Policies.
12.3. In the event that the ENTX Information Technology Administrator judges that an account on one of the multi-user computing systems presents an immediate security risk, the ENTX Information Technology Administrator may deactivate the computer account without prior notice.

13.**Password Policy**

13.1. Password Creation
13.1.1. ENTX personnel are responsible for choosing strong passwords and keeping them confidential, secure or locked away in a secure area.
13.1.2. Passwords must meet complexity requirements and contain three of the following:

- Must contain upper and lower case characters
- Must contain numeric characters
- Must NOT contain a number as the first or last character
- Must NOT contain any word greater than 3 letters found in a dictionary

- May contain punctuation marks

13.1.3. Must not be a password you have used during the 365 days
13.1.4. Must not be one of the last 24 passwords you have used
13.1.5. Minimum password length is 8 characters.
13.1.6. Account lockout threshold initiates after 6 invalid logon attempts within 14 minutes.
13.1.7. Account lockout duration is 15 minutes.
13.1.8. User logon restrictions are enforced.
13.1.9. Users must not use the same password for TTU accounts as for other non-TTU access (for example, personal ISP accounts, online banking accounts, personal email accounts, etc.).

13.2. Password Protection

13.2.1. Passwords must not be shared with anyone. All passwords are to be treated as sensitive, confidential ENTX information.
13.2.2. Passwords must not be inserted into email messages or other forms of electronic communication.
13.2.3. Passwords must not be revealed over the phone to anyone.
13.2.4. Do not reveal a password on questionnaires or security forms.
13.2.5. Do not hint at the format of a password (for example, “my family name”).
13.2.6. Do not share ENTX passwords with anyone (co-workers, management, etc.) while you are on vacation or away from the office.
13.2.7. Do not write passwords down and store them anywhere in your office.
13.2.8. Do not store passwords in a file on a computer system or mobile device (phone or tablet) without encryption.
13.2.9. Do not use the “Remember Password” feature of applications (for example, web browsers).
13.2.10. Any user suspecting that his/her password may have been compromised must report the incident and change all passwords.

13.3. Administrator Passwords

13.3.1. To prevent unauthorized administrative access to ENTX servers, the ENTX Information Technology Administrator maintains all administrative passwords, which are known only to select IT personnel who at a minimum has been vetted by the University criminal background check.
13.3.2. Should a breach of ENTX server security occur, the administrator passwords will be immediately changed and an investigation of how the breach occurred will be conducted.
13.3.3. Such a password breach is a security violation of ENTX resources and will be brought to the attention of the proper authorities for full prosecution under the law.

14. Personnel Communication Devices Policy

14.1. Issuing Policy

14.1.1. Personnel Communication Devices (PCDs) can be issued to ENTX personnel with duties that require them to be in immediate and frequent contact when they are away from their normal work locations.
14.1.2. For the purpose of this policy, PCDs are defined to include handheld wireless devices, cellular telephones, laptop wireless cards and pagers.
14.1.3. Handheld wireless devices may be issued to personnel who need to conduct immediate, critical ENTX business.

14.2. Bluetooth
14.2.1. Hands-free enabling devices, such as Bluetooth, may be issued to authorized ENTX personnel. Care must be taken to avoid being recorded when peering Bluetooth adapters (for example, Bluetooth 2.0 Class 1 devices have a range of 330 feet).
14.3. Voicemail
14.3.1. Voicemail boxes of ENTX personnel must be protected by a PIN which must never be the same as the last four digits of the telephone number of the voicemail box or contain any digits of your Social Security Number.
14.4. Loss and Theft
14.4.1. Files containing confidential or sensitive data may not be stored in PCDs unless protected by approved encryption.
14.4.2. Un-encrypted confidential or sensitive data shall never be stored on a personal PCD.
14.4.3. Lost or stolen equipment must immediately be reported to the ENTX Information Technology Administrator and the ENTX Quality Assurance/Safety Manager
14.5. Personal Use
14.5.1. PCDs and voicemail are issued for ENTX business. Personal use should be limited to minimal and incidental use.
14.6. PCD Safety
14.6.1. Conducting telephone calls or utilizing PCDs while driving can be a safety hazard. Drivers should use PCDs while parked or out of the vehicle.
14.6.2. If employees must use a PCD while driving, ENTX Information Technology Administrator requires the use of hands-free enabling devices.

15. **Server Policy**

15.1. General Requirements
15.1.1. The ENTX Information Technology Administrator maintains all access and data stored on the ENTX servers.
15.1.2. The ENTX servers are in a locked room on site with restricted access.
15.1.3. The ENTX servers are located on the TTU network behind the University firewall and intrusion detection system to protect against unauthorized intrusion.
15.1.4. All ENTX servers are configured to provide built-in redundancy that protects data against loss of any one hard disk. Should a hard disk fail, the hard disks have the capability to be hot swapped without shutting down the server.
15.1.5. To prevent total data loss, should a complete server failure occur, the ENTX servers are backed-up on a nightly basis. These backups are stored on the ENTX storage arrays located on site in a locked room with restricted access. The ENTX storage arrays also have the ability for hot swapping the hard disks.
15.2. Configuration Requirements
15.2.1. Services and applications that will not be used must be disabled where practical.
15.2.2. Security patches and updates will be applied after thorough testing.
15.2.3. The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with ENTX business.
15.2.4. Always use the least required access privilege to perform a function.
15.2.5. Servers must be physically located in an access-controlled environment.

16. Technology Equipment Disposal Policy

16.1. Technology equipment refers to desktops, laptops, tablets or netbooks, printers, copiers, monitors, servers, handheld devices, telephones, cell phones, disc drives or any storage devices, network switches, routers, wireless access points, battery backups, backup hard drives and tapes, etc.
16.2. When ENTX technology assets have reached the end of their useful life they must be given to the ENTX Information Technology Administrator for proper disposal.
16.3. The ENTX Information Technology Administrator will securely erase all storage mediums.
16.4. All electronic drives must be degaussed or overwritten with a disk cleaning program. Hard drives will be removed and rendered unreadable (drilling, crushing or other demolition methods).
16.5. All data including, all files and licensed software shall be removed from equipment using disk sanitizing software that cleans the media overwriting each and every disk sector with zero-filled blocks.
16.6. No technology equipment can be sold to another individual or entity.
16.7. Technology equipment with non-functioning memory or storage technology will have the memory and/or storage removed and it will be physically destroyed.

17. Unauthorized Software Policy

17.1. ENTX personnel are responsible for all data and computing programs downloaded on their ENTX issued computers and personal computers brought onto the ENTX premises and connected to the TTU network.
17.2. Examples of unauthorized software include, but are not limited to, the following:

- FTP and Telnet file transfer programs
- Network scanning tools or programs
- Network sniffing tools or programs
- Password cracking software
- Peer-to-peer software
- Any software that is not properly licensed
- Any software used for illegal download of music, movies, etc.

18. Training

18.1. ENTX information technology security training will be provided on a yearly basis.
18.2. Refresher trainings will be provided on an as needed basis and / or new technologies are introduced.
18.3. Examples of topics in the training program but not limited to include:
18.3.1. Physical Security
18.3.1.1. Protecting the physical area and equipment (i.e., locking doors, security file cabinets, caring for CD's / DVD's, USB's, etc.).
18.3.2. Sharing of unique means of access
18.3.2.1. Reporting of loss or compromise of passwords.
18.3.2.2. Protecting passwords or other authentication data devices (i.e., never divulge passwords, PIN's, etc.).
18.3.2.3. Reporting of suspicious person or activities.

18.3.2.4. Reporting security violations or incidents (i.e., who to call if a computer virus is suspected).
18.3.3. Information systems control
18.3.3.1. Control of external connections to facility security systems (who's responsible).
18.3.3.2. Only authorized and authenticated users to information, files and equipment is granted to approved personnel.
18.3.3.3. Controls are in place designed to prevent malicious code (who's responsible).

19. Virtual Private Networking (VPN) Policy

19.1. Virtual Private Networking (VPN) provides off-campus users a secure connection to the TTU network. The use of VPN provides firewall and Intrusion Detection System (IDS) protections afforded on-campus users of the TTU network.
19.2. VPN is required when accessing ENTX information from any portable device away from the TTU network. Examples of portable devices include, but are not limited to, the following:

- Desktops / Laptops
- Tablet devices
- Smartphones
- Future technology development

19.3. It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access the ENTX servers.
19.4. All computers connected via VPN must use the most up-to-date anti-virus software provided by the ENTX Information Technology Administrator.

20. Workstation Security for HIPAA Policy

20.1. ENTX employees using ENTX workstations shall consider the sensitivity of the information, including protected health information (PHI) that may be accessed and minimize the possibility of unauthorized access.
20.2. ENTX will implement physical and technical safeguards for all workstations that access electronic protected health information to restrict access to authorized users.
20.3. Appropriate measures include:

- Restricting physical access to workstations to only authorized personnel.
- Securing workstations (screen lock or logout) prior to leaving area to prevent unauthorized access.
- Enabling a password-protected screen saver with a short timeout period to ensure that workstations that were left unsecured will be protected. The password must comply with the TTU *Password Policy.*
- Complying with all applicable password policies and procedures.
- Ensuring workstations are used for authorized business purposes only.
- Never installing unauthorized software on workstations.
- Securing laptops that contain sensitive information by locking laptops up in drawers or cabinets.
- Installing privacy screen filters or using other physical barriers to alleviate exposing data.
- Exit running applications and close open documents.