

TTUHSC IT Policies

INTRODUCTION

The purpose of implementing Information Technology (I.T.) policies and standards is to establish a common framework for adopting and deploying [Information Technology resources](#) within the Texas Tech University Health Sciences Center (TTUHSC) environment.

These policies and standards have been established in order to:

- Provide constituents with an integrated I.T. environment that supports the mission of TTUHSC
- Safeguard the privacy, confidentiality, and reliability of data
- Protect and maximize TTUHSC's investment in I.T. resources
- Reduce TTUHSC's business and legal risks, and
- Define the responsibility and the requirements for the use of I.T. resources within the TTUHSC environment

TEXAS TECH UNIVERSITY SYSTEM BOARD OF REGENTS POLICIES AND INSTITUTION OPERATING POLICIES AND PROCEDURES

The Texas Tech University System Board of Regents (BOR) is the governing board of this Institution. The Board has promulgated policies which are found in the [Rules and Regulations of the Board of Regents](#).

The President of Texas Tech University Health Sciences Center (TTUHSC) is also authorized by the Board to promulgate policies, which are found in the [TTUHSC Operating Policies and Procedures Manual](#). These policies may either implement or interpret Board policies, or are independent statements of policy which are consistent with BOR policies.

I.T. policies are drafted by the Technical Advisory Council (TAC), which is made up of I.T. representatives from each campus and school. With the approval of the Chief Information Officer (CIO), the draft policy is forwarded to the I.T. Board of Directors for review and comment. After the I.T. Board of Directors' review, the CIO will forward the proposed policy to the President for consideration and approval.

Under the authority defined in [TTUHSC Operating Policy 56.01, Use of Information Technology Resources](#), I.T. policies and procedures are located at <http://www.ttuhscc.edu/IT/Policy>.

Related BOR Policies and TTUHSC Operating Policies and Procedures include but are not limited to:

- [Rules and Regulations of the Board of Regents, Chapter 10 - Intellectual Property Rights](#)
- [TTUHSC OP 10.05 - Confidentiality and Employee Information Privacy](#)
- [TTUHSC OP 57.02 - Guidelines for the Educational Use of Copyrighted Works](#)
- [TTUHSC OP 61.01 - Private Use of State Property](#)

1. SECURITY

1.1. IT. RESOURCE MANAGEMENT AND RESPONSIBILITIES (TAC 202.71, 202.72)

Information Security Program

Each state agency head or his or her designated representative(s) shall designate an [Information Security Officer \(ISO\)](#) to administer the state agency Information Security Program. The ISO shall report to executive level management. TTUHSC's Information Security Program will be reviewed annually for compliance with [TAC 202](#) standards. Other responsibilities of the ISO include the following:

- - Document and maintain an up-to-date information security program. The information security program shall be approved by the institution of higher education head or his or her designated representative(s).
 - Develop recommended policies and establish procedures and practices, in cooperation with information owners and custodians, necessary to ensure the security of information resources assets against unauthorized or accidental modification, destruction or disclosure.
 - Monitor the effectiveness of defined controls for mission critical information.
 - Report, at least annually, to the institution of higher education head or his or her designated representative(s) the status and effectiveness of information resources security controls.
 - Issue exceptions to information security requirements or controls in this chapter. Any such exceptions shall be justified, documented, and communicated as part of the risk assessment process.
 - Work with the [owners](#) of information resources to develop strategies to meet their required responsibilities and to ensure compliance.

Defined Responsibilities

Information Owner Responsibilities – the owner or their designated representative(s) are responsible for and authorized to:

- Approve access and formally assign custody of an information resources asset
- Determine the asset's value
- Specify data control requirements and convey them to users and custodians
- Specify appropriate controls, based on a risk assessment, to protect the state's information resources from unauthorized modification, deletion, or disclosure. Controls shall extend to information resources and services outsourced by the institution of higher education.
- Confirm that controls are in place to ensure confidentiality, integrity, and availability of data and other assigned information resources.
- Assign custody of information resources assets and provide appropriate authority to implement security controls and procedures
- Review access lists based on documented security risk management decisions

- Approve, justify, document and be accountable for exceptions to security controls. The information owner shall coordinate exceptions to security controls with the ISO or other person(s) designated by the state institution of higher education head.
- Classify business functional information

Custodians of information resources shall:

- Implement the controls specified by the owner(s),
- Provide physical, technical, and procedural safeguards for the information resources,
- Assist information owners in evaluating the cost-effectiveness of controls and monitoring, and
- Implement monitoring techniques and procedures for detecting, reporting, and investigating incidents.

User Responsibilities - the user of the information resources is responsible for:

- Using the resources only for the designed purpose, and
- Complying with the controls specified by the owner(s).
- Information system owners, in collaboration with the Information Security Officer or designee, shall assess a risk level based on the inherent risk with a ranking of “High”, “Medium”, or “Low”. The criteria for each level are:

High Risk	Medium Risk	Low Risk
Involve large dollar amounts, or significantly important information that would impact the operations of the HSC, or	Involve a moderate or low dollar value, or	Generally available public information, or
Contain confidential or sensitive data, or	Information that could potentially create problems for the parties involved, or	Result in a relatively small impact for the HSC
Impact a large number of people or networks	Impact a moderate portion of the Institution’s customer base	

- See [Policy 1.4.1](#) for further responsibilities.
- A system change could cause the overall classification to move to another risk level

Managing Security Risks

A [security risk analysis](#) of information resources shall be performed and documented on the following schedule:

- Annually on information resources classified as high risk
- Biennially on information resources classified as medium or low risk

Security risk assessment results, vulnerability reports and other security analysis information shall be presented to the President of the HSC or their designated representative(s). The President of the HSC or designated representative(s) shall make the final security [risk management](#) decisions to either accept the risks or to modify the security and controls for the information resources based on its value and sensitivity. The President of the HSC or their designated representative(s) must approve the final security risk management plan.

[1.2 MANAGING PHYSICAL SECURITY \(TAC 202.73\)](#)

Access to I.T. Data Centers will be documented and controlled. Only authorized personnel will have access to any Institutional Data Center. An annual review of the physical security measures of the Data Centers will be conducted by the Information Security Officer. Data Center personnel will be trained to monitor environmental controls and trained in appropriate responses to emergencies or equipment problems. Appropriate safety procedures, as defined by the Safety Services Department and outlined in the I.T. Division's Disaster Recovery Plan will be followed and annual tests conducted.

1.3 DISASTER RECOVERY ([TAC 202.74](#))

This policy sets forth the guidelines and procedures for recovering the Data Center and all related information systems providing service to the Institution. In accordance with the [Texas Administrative Code Rule §202.72](#), Business Continuity Planning, the I.T. Division shall develop and maintain a Disaster Recovery Plan (DRP) that delineates all the roles and responsibilities for the individual Disaster Recovery Teams, along with the steps that must be taken for successful recovery operations.

At a minimum, the DRP shall be tested annually or when a major revision occurs and I.T. staff assigned to disaster recovery duties shall be trained, at least, on an annual basis.

In the event of a disaster,

- The Chief Information Officer (CIO) is the only authority for declaring a disaster for the Data Center and all related I.T. services based on the findings of the Tactical Operations Team.
- The Tactical Operations Team is responsible for the timely identification and determination of the disaster as well as the duration of the service outage.

Upon the declaration of a disaster,

- The I.T. Division and all associated Disaster Recovery Teams will invoke and comply with the procedures documented in the DRP.
- All efforts will be made to accommodate user needs while recovery services are being implemented but prioritization of recovery will be based on the criticality of the service and/or application experiencing the outage.
- The Office of Communications and Marketing is the only authority for all media communications based on information from the Chief Information Officer.

- The Chief Information Officer or designee from the Management Team is responsible for conveying all necessary information to the Office of Communications and Marketing for any updates and/or announcements to the media.

Mission Critical data shall be backed up on a scheduled basis and stored off site in a secure, environmentally safe, locked facility accessible only to authorized personnel.

TTUHSC Information Resources backup and recovery process for each system must be documented and periodically reviewed. A process must be implemented to verify the success of the electronic information backup.

Backups must be periodically tested to ensure that they are recoverable.

1.4 Security Safeguards (TAC 202.75.7)

1.4.1 ACCEPTABLE USE

Conduct Yourself Responsibly

The use of TTUHSC I.T. resources may be temporarily or even permanently revoked at any time for abusive conduct. Such conduct includes placing unlawful information on a system, copyright violations, using abusive or otherwise objectionable language in either public or private messages, sending messages that are likely to result in the loss of recipients' work or systems, sending unauthorized messages to individuals, or any use that would cause congestion of the networks or otherwise interfere with the work of others.

Use of peer-to-peer programs on TTUHSC computers and/or network for downloading and/or uploading of illegal copies of copyrighted media is strictly prohibited. All students, faculty, and staff should remove these applications immediately from TTUHSC computers. Students, faculty, and staff who use their personally-owned computers to connect to the TTUHSC network must disable all peer-to-peer applications and services before connecting to the network. This includes direct connection or remote connection via [PPP](#), [VPN](#), or wireless accounts. Any computers using peer-to-peer applications on the TTUHSC network are subject to removal from the network until the application is removed or disabled.

Misuse of TTUHSC information resources is a violation of the policies contained herein and will result in disciplinary action in accordance with HSC OP's [70.31](#) and [77.05](#) and the [Student Affairs Handbook](#).

Computing Ethics And User Responsibilities

Information technology resources at TTUHSC are owned by the State of Texas and administered by the Information Technology Division. All products created on Institutional property belong to the Institution. These products shall be considered "intellectual property" as defined by and managed according to [Board of Regents Rules and Regulations, Chapter 10 - Intellectual Property Rights](#). TTUHSC will provide access to appropriate central and campus I.T. resources, and to their attached networks to all members of the TTUHSC community. Users are

responsible for managing their use of I.T. resources and are accountable for their actions relating to information technology security.

General Principles

Users must abide by the following list of standards that have been established:

1. Report any weaknesses in TTUHSC computer security, any incidents of possible misuse, or violation of these policies to the appropriate I.T. management.
2. Access only information that is your own, that is publicly available, or to which you have been given authorized access. Users may use only the I.T. resources they are authorized to use and only for the purposes specified when their accounts were issued or permission to use the resources was granted.
3. For security reasons, protect your USER ID, password, and system from unauthorized use. Users who share their access with another individual shall be responsible and will be held accountable for **ALL** usage of their accounts.
4. Use only legal versions of copyrighted software in compliance with vendor license requirements. Users shall not transport software provided by TTUHSC to another computer site without prior [authorization](#) from the departmental administrator. To do so constitutes theft.
5. DO NOT attempt to circumvent or subvert system, network, destroy the integrity of computer-based information, or access controlled information on the TTUHSC network.
6. DO NOT install software/hardware for personal use on TTUHSC systems.
7. Sexually explicit material in any form is not allowed on TTUHSC systems. See [Sexually Explicit Material section](#) for more detailed guidelines.
8. Users must not unreasonably interfere with the fair use of I.T. resources by another. Examples of unreasonable interference include playing games, listening to or viewing streaming audio/video for recreation, intentionally misconfiguring or tampering with videoconferencing equipment, interfering with the scheduled use of a [distance learning classroom](#) by failing to promptly vacate the room at the end of a session, and intentionally running a program that attempts to violate the operational integrity of the TTUHSC network.
9. Users are prohibited from using the TTUHSC's systems or networks for personal or commercial gain, such as, selling access to your USER ID or to TTUHSC systems or networks, performing work for profit with TTUHSC resources in a manner not authorized by the TTUHSC, marketing/advertising, and/or personal business transactions with commercial organizations.
10. TTUHSC systems are not to be used for partisan political purposes, such as using electronic mail to circulate advertising for political candidates or lobbying of public officials.
11. DO NOT use mail or messaging services to harass or intimidate another person, for example, by broadcasting unsolicited messages, or by repeatedly sending unwanted mail.

The above list is by no means exhaustive, but attempts to provide a framework for activities that fall into the category of unacceptable use.

Sexually Explicit Material

Users shall not view, retrieve, transmit, distribute, print, or save any electronic files that may be deemed sexually explicit on TTUHSC I.T. resources. This includes both visual and textual sexually explicit material as defined by [Chapter 43 of the State of Texas Penal Code on Public Indecency](#). Exceptions are material used for scientific, medical, and/or educational purposes.

It is also illegal to use sexually explicit material to intimidate, persecute, or otherwise harass another individual. This is considered sexual harassment. For more detailed guidelines on sexual harassment, refer to [HSC OP 70.14](#).

Do not open any emails which you believe to contain obscenity or pornography. If obscenity and/or pornography are received through email, there will be no disciplinary proceedings if the mail is deleted immediately. If the offending email originates from a TTU or TTUHSC email address, report the receipt of said material to the [Assistant Vice President for Human Resources](#) and/or the [Information Security Officer](#) immediately. Reporting of such a violation will be held in the strictest confidence.

1.4.2 ACCOUNT MANAGEMENT AND USER RESPONSIBILITIES

eRaider is an account management system which makes it possible for students, faculty, and staff to obtain and access electronic resources at Texas Tech using a single username and password. Your eRaider username and password are required to access many of these resources. An eRaider account is required to access the TTUHSC domain. New students, faculty, and staff receive an eRaider account upon coming to the Health Sciences Center; access is dependant upon account types (i.e. faculty, staff, and students) and department requirements. Questions regarding eRaider account information should be directed to the [I.T. Solutions Center](#) at each respective campuses.

1.4.3 ADMINISTRATOR/SPECIAL ACCESS

This policy provides a set of requirements for the regulation and use of administrator or special access on the TTUHSC systems. This policy will provide a mechanism for the addition and removal of people from special access in the Active Directory domain and a mechanism for periodic reviews of the administrator/special access database.

Special Access will need to be requested by the information owner or designee and submitted to the I.T. Solution Center at <http://www.ITSolutions.ttuhsc.edu>

Regulation of Special Access Accounts:

1. Special access on TTUHSC system is maintained and monitored by both Data Center Operations and the Information Security Officer.
2. Passwords for special access accounts are changed on a regular basis as determined by Institutional policy.
3. Special access is only provided to individuals who need the access to perform their job.

4. Any misuse of special access privileges must be reported to the TTUHSC Information Security Officer when discovered.
5. Persons requesting special access must follow all procedures outlined in the Special Access Guidelines.
6. Persons who misuse their special access privilege can have special access revoked and may face Institutional disciplinary action (See [Policy 10 - Disciplinary Process](#))
7. Special access is reviewed on a periodic basis as defined below.
8. All persons who currently (prior to the approval of this policy) have special access are required to submit a completed Special Access Request form and a signed Special Access Guidelines agreement.

Performing a Periodic Review of the Special Access Database

A review of special access will be made on an annual basis or as determined by the TTUHSC Information Security Officer. The review process will involve the following steps:

- A report will be generated from Active Directory. The report will list: special access by system and access type; and access by person (i.e., for each person, all access given to that person is listed).
- The reports will be distributed to the Information Security Officer, the Manager of the Data Center, and the manager of users given special access. Each person reviews the list (or appropriate part of) to determine if any changes should be made.
- Should anyone determine that an individual needs to be added to other special access groups, that individual must submit a Special Access Request form requesting the additional access.
- If there are any deletions to be made to the permissions, the Manager of the Data Center will make the appropriate changes.

Special Access Guidelines

This agreement outlines the use of special access on TTUHSC computers. Special access is defined as having domain access other than as a domain user. The TTUHSC environment is very complex and dynamic. Due to the number and variety of computers and peripherals, special access must be granted to numerous people so the TTUHSC facility can be properly supported. People with special access must develop the proper skill for using that access responsibly.

The Special Access Guidelines have been developed to help people to use their special access in a responsible and secure manner. All persons requesting special access must read and follow these guidelines.

General Guidelines

1. Be aware of your TTUHSC computing environment.
2. Always log on systems where you have an account as yourself. Any action done under a special access account should have an audit trail.
3. Use special access only if necessary.

4. Many system tasks require the use of root or other special access. However, there are many tasks that can be done without the use of special access. When at all possible use regular accounts for trouble-shooting and investigating.
5. Complete the appropriate Change Request processes specified in Section 1.4.5. Document all major actions and/or inform the appropriate people.
6. Documentation provides a method to analyze what happened. In the future, others may want to know what was done to correct a certain problem. The Lead System Analyst or Manager of the Data Center is to be informed BEFORE any changes are made to system specific or configuration files.
7. Have a backup plan in case something goes wrong. Special access, especially root or administrative access has a large potential for doing damage with just a few keystrokes. You must be able to restore the system to its state before the error occurred.
8. With the use of special access, situations arise that have never come up before. Although TTUHSC has many written procedures, they do not cover every circumstance possible. If any doubt exists about how you should proceed on a problem, ask for assistance.

Specific Considerations Regarding Special Access

1. Do not share special access passwords with anyone.
2. Do not write down the special access passwords or the current algorithm.
3. Do not routinely log onto a system for which you have an account, as “root” or any other special access account.
4. Do not read or send personal mail, play games, read the net news or edit personal files using a special access account.
5. Do not browse other user’s files, directories or email using a special access account.
6. Do not make a change on any system that is not directly related to your job duties. The TTUHSC System Administration Handbook states “The Lead System Analyst is responsible for approving all changes to the systems(s) of his/her responsibility. No changes are to be made to any system configuration file or executable file without prior approval of the Lead System Analyst and Manager of the Data Center.” Making a change AND then informing the Lead System Analyst is considered a violation of this guideline.
7. Do not use special access to create temporary files or directories for your own personal use.

1.4.4 BACKUP/RECOVERY

Shared resources (i.e. Network File Shares) are the primary method of protecting Institutional data. Non-business related data must not be stored on shared resources and is subject to deletion.

Departments are responsible for the creation of electronic and/or paper copies of institutional data and retention of that institutional data as defined by the [Records Retention Operating Policy, 10.09](#). Disaster Recovery backups are not considered a valid retention mechanism for records retention purposes and must not be used by departments to meet records retention requirements.

Institutional server backups are performed for disaster recovery purposes only. Institutional servers are backed up based on the schedule listed below.

Nightly - Incremental backups will be performed to be retained until the next full backup is performed.

Weekly - Full data backups will be performed to be retained for four weeks.

Per disaster recovery best practices, backup tapes are stored off-site. The details of the off-site storage are outlined in the I.T. Division Disaster Recovery Plan.

Data Restoration

Shared resource data may be restored provided the backup is within the storage timeframe as defined above. Restoration of shared resource data may be requested through the [I.T. Solutions Center](#) work order process.

Email Retention

Email backups are for disaster recovery purposes only. Restoration of individual email boxes is not possible.

Email in the Deleted Items folder will automatically be permanently deleted 15 days after the email is placed in the Deleted Items folder.

Email in the Junk E-mail folder will automatically be permanently deleted 30 days after receipt.

Permanently deleted (either automatically because of retention dates or manually by the user) email is recoverable by the end user for 21 days from the date of permanent deletion using Outlook Tools or Outlook Web Access.

1.4.5 CHANGE MANAGEMENT

Change Definition

The following change management protocols apply to the Institutional IT units as well as the regional campuses' IT departments. The IT Division highly recommends that all departments adopt these industry best practices related to IT change management in their respective areas. A change is defined as a modification to the hardware, software, and documentation managed by Information Technology that has a reasonable possibility of impacting normal operations of those resources. Items that are considered changes include, but are not limited to:

- Installation or upgrades of server, networking, or security hardware or software, including patches and interim fixes,
- Modification of hardware or software that affects the operation of desktop computers connected to the TTUHSC network,

- Modification of server, network, or security settings that affect access to I.T. resources, and
- Modification or enhancements to the physical environment that supports I.T. resources.

Specific tasks that should not be considered changes include:

- Creation of new file shares, or modification to permissions of existing shares,
- Installation, activation, or removal of network cable drops, or
- Creation, modification, or deletion of accounts and mailboxes.

Change Categories

Changes will be classified into three categories:

- Category 1 - This category includes changes to resources that provide service to a large number of internal or external I.T. customers, or customers at multiple regional locations.
- Category 2 - This category includes changes to resources that provide service to a moderate number of I.T. customers within a specific location.
- Category 3 - This category includes changes for a single department or smaller group of users at a specific location.

Procedures

All changes must be documented, and submitted for approval prior to implementation. The following defines the procedure for documentation and approval.

Documentation

The requester initiating the change must initiate a Request Creator process via the STARS system (<http://www.ttuhs.edu/IT/STARS/roles/default.aspx>). The following information must be provided on this form:

- Submission date - Date the change form is submitted for approval,
- Change date and time - Proposed date and time the change will be performed,
- Change duration - Estimated length of time for the change to be completed,
- Control Number - Change Identification number which uses the date of the request and a sequential number for multiple requests originated on the same date starting with 001 in the following format: YYYYMMDD-NNN,
- Change category - See prior section for definition,
- Change Purpose - Fifty character summary of the Change Description,
- Change description - Explanation of the change,
- Impact description - Campus and departments or groups of customers that will be affected by the change,
- Test procedure - Description of the testing performed for the change, if applicable,
- Back-out procedure - Procedure for backing out the change if the implementation is not successful, and

- Back-out duration - Estimated time to back out the change.

The technician's manager will record the change request in a common Change Request Log maintained by the Managing Director of Network, Security, and Systems.

Processing

After the requester completes the Change Approval Form, it will be submitted to their supervisor or manager for review/approval. The approver will ensure the form is completed and information provided is adequate for decision making. The managers will meet with the authorized approver for Network Services, Information Security, Systems, or schools as needed to review and document recommendations. Change forms must be submitted to the approver of the applicable areas a minimum of one full business day prior to the review date.

If the authorized approver is unavailable for the weekly meeting, the managers will meet to discuss and make recommendations for the change requests. The authorized approver must be notified of all category 1 and 2 changes before implementation.

All changes will be forwarded to I.T. Executive Management (consisting of the CIO, AVP of Information Services, AVP of Security and Infrastructure Assurance, and Managing Director of Technology Services) for final disposition of the request.

Category 1 and 2 changes can be implemented no sooner than two full business days after approval. Category 3 changes can be implemented immediately after approval, according to the change date and time on the approval form.

Announcement messages must be distributed prior to all category 1 and 2 changes. Message content should include impact to user and training provided if applicable. The supervisor or manager should prepare this announcement prior to the change review meeting. The authorized approver will be responsible for posting the announcement.

Changes that are backed out during or immediately after implementation must be resubmitted for approval.

Emergency Changes

Occasionally, it may be necessary to implement changes before the next weekly change approval meeting. These changes will be designated as emergency changes, and will be documented as Emergency (E) Category, a category E1, E2, or E3.

All of the above documentation and approval procedures still apply for emergency changes, except these changes can be immediately submitted to the supervisor, and subsequently the CIO, for approval and implementation.

Emergency change requests should only be submitted when I.T. operations or security will be negatively impacted or compromised if the change is not implemented immediately.

1.4.6 EMAIL

All Institutional email services will be delivered using the Microsoft Exchange platform. The supported email client is Microsoft Outlook or the web-based Outlook Web Access.

TTUHSC email accounts are available dependant on the type of associated HSC affiliation. The creation of email accounts are provisioned through the eRaider account activation process and online eRaider Account Manager. Assistance with eRaider and HSC eMail account setup can be obtained through the department hiring managers and the [I.T. Solutions Center](#).

The volume of unsolicited bulk email (SPAM) that is received negatively impacts the Institution's infrastructure and productivity. Therefore, the Institution has deployed infrastructure to reject a high volume of SPAM emails before they are processed by our email servers. Additional infrastructure has also been deployed for students, faculty, and staff to use on their personal computers. For assistance or more information on strategies to manage SPAM/Junk Email, please contact the I.T. Solutions Center or go to <http://www.ttuhs.edu/it/helpdesk/anti-spam.aspx>.

Email Naming Convention

The approved email-addressing format uses the firstname.last/surname@ttuhsc.edu naming convention (e.g. john.doe@ttuhsc.edu). This will be the official TTUHSC email address format for all students, faculty, and staff.

The naming convention for people who share the same name is slightly different. If a name already exists in the email database, a variation will be used, such as firstname.middleinitial.last/surname@ttuhsc.edu format (e.g., john.s.doe@ttuhsc.edu).

The CIO or their designee is the central authority for username and email address assignments for all campuses. Any disputes over usernames and/or email addresses should be referred to the CIO or their designee for resolution.

Users wanting to verify their email address can call the following numbers:

Lubbock Information Technology Solutions Center - (806) 743-1234

Amarillo Information Technology Help Desk - (806) 354-5404

El Paso Information Technology Help Desk - (915) 545-6800

Odessa Information Technology Help Desk - (432) 335-5108

To ensure Institution business is not disrupted, all business cards, stationery, and any other correspondence material must reflect the correct email address format, including contact information on web sites. All students, faculty, and staff should only use their official TTUHSC

email address to facilitate the dissemination of information as well as promote and sustain the lines of communication.

Because email addresses are printed on official stationery, business cards, or any other correspondence material, all print jobs and/or official publications must follow the Publication Guidelines as established by the Office of News and Publications. Refer to [HSC OP 67.01](#) (Publication Guidelines) for detailed guidelines on printing standards.

Implementation And Compliance Procedure

All TTUHSC students, faculty, and staff will be issued an official TTUHSC email account with the firstname.last/surname@ttuhsc.edu naming convention format. This email address will be the only email address used for all official communications between the Institution and students, faculty, and staff. Emails will not be redirected or forwarded to another, non-TTUHSC account.

Sending Confidential Information

Any emails containing confidential information that are sent to persons outside TTUHSC or TTU must be encrypted. For more information regarding confidentiality and encryption please reference [Operating Policy 56.04](#). For further instructions, go to www.ITsolutions.ttuhsc.edu.

Correspondences containing vital Institutional information must include the following disclaimer at the end of the email:

Confidentiality Notice: This message, including any attachments, is for the sole use of the intended recipient(s) and may contain confidential and privileged information. Any unauthorized review, use, disclosure, or distribution is strictly prohibited. If you are not the intended recipient, please contact the sender by reply e-mail and destroy all copies of the original message.

Mass Email

TTUHSC mass email messages must be approved by the President, Vice Presidents or Deans for distribution of suitable email to TTUHSC schools, campuses and institution. For the purpose of student mass email communication, a designated representative of Student Services can also distribute mass email to students, with email content that is considered creditable and informative, that does not include commercial interest.

Suitable mass email material for approval includes, but is not limited to:

- Substantial changes in governance, policy, or practice
- Immediate threats to health, safety, property, or research
- Infrastructure maintenance, computer or telecommunication issues

- Official non-commercial survey material, institutional newsletter publications
- Institutional newsletter publications

The preferred method of communicating with all members of the schools, campuses and institution, which is not viewed as appropriate material for mass email communication, is through announcement web pages, institutional news article releases, mailing material, leaflets, brochures and notice boards.

To facilitate official mass email communication, Information Technology maintains the resources for email address groups. Access to send to these groups is restricted to approved representatives only from the governing authorities. Attempting to send mass email communication to TTUHSC members and groups, which has not been approved by the appropriate authority, is in violation of IT Policy, [1.4.1 Acceptable Use](#).

Alumni and Retiree Email Accounts

Official TTUHSC email accounts are only issued to current TTUHSC students, faculty, and staff. After the owner's biographical record ceases to be supplied from Personnel Records, Student Records, or other approved sources, the eRaider Account Manager will automatically disable access to HSC eMail. Individuals should make plans to transfer their email to another location prior to graduation or last day of employment.

Graduating students who would like to continue to receive information from TTUHSC are strongly encouraged to register themselves at www.RaiderCheckUp.com. Users needing help registering on the site should call the Alumni Relations Office at (806)743-3238 or email TTUHSCAlumni@ttuhsc.edu

1.4.7 INCIDENT MANAGEMENT

The following describes the requirements for managing [security incidents](#). Security incidents include, but are not limited to detection of viruses, worms, and Trojan horses, unauthorized use of computer accounts and computer systems, as well as complaints of improper use of information resources as outlined in the [Acceptable Use Policy](#).

Responsibilities

TTUHSC [Information Technology Security \(ITS\) group](#), in coordination with the [Computer Incidence Response Team \(CIRT\)](#) members is responsible for the following:

- developing and preserving the procedures for handling incidents,
- defining and classifying incidents,
- determining the tools and technology utilized in intrusion detection,
- determining if an incident should be investigated and the scope of such an investigation (i.e. law enforcement agencies, forensic work),
- securing the network,

- conducting follow-up reviews,
- insure the proper reporting is conducted, and
- promoting awareness throughout the organization.

Standard/Procedure

1. TTUHSC CIRT members may be required to perform duties related to the incident that take precedence over normal duties.
2. The Information Security Officer is responsible for:
 - a. initiating incident management action, including notifying the appropriate personnel.
 - b. determining the physical and electronic evidence to be gathered as part of the incident investigation.
 - c. determining if a widespread TTUHSC conference call is required, the content of the conference call, and how best to contact CIRT members
 - d. initiating, completing, and documenting the incident investigation with assistance from the CIRT
 - e. coordinating communications with outside organizations and law enforcement.
 - f. reporting the incident to the:
 - CIO or their designee
 - [Information Technology Security Council](#)
 - Managing Director of Technology Services
 - State of Texas Department of Information Resources
3. The appropriate technical resources from the CIRT are responsible for:
 - a. ensuring that any damage from a security incident is repaired or mitigated, and that the vulnerability is eliminated or minimized where possible.
 - b. communicating new issues or vulnerabilities to the system vendor and working with the vendor to eliminate or mitigate the vulnerability.
4. In the case where law enforcement is not involved, the Information Security Officer will provide the appropriate information to the Managing Director of Technology Services, who will notify TTUHSC Human Resources as appropriate.
5. In the case where law enforcement is involved, the CIO is responsible for reporting the incident to Federal, State, or local law officials as required by applicable statutes and/or regulations as well as act as the liaison between law enforcement and TTUHSC.

Guidelines For Handling A Computer System Incident

Don't panic. Call the I.T. Help Desk. The Help Desk staff will guide you through the next steps to take, which includes the following:

1. **Assessment.** Do not immediately shut down the machine, as you may lose important information. If the machine is being used to attack others, or if the attacker is actively using or damaging the machine, you may need to disconnect it from the network. If this does not appear to be the case, leave the system intact for the moment.

2. **System scan.** Work with the I.T. Help Desk and run an emergency system security scan. This information will help you assess the damage. (The machine must be up and on the network in order to run a scan.)
3. **Gathering all relevant information.** This may include, but is not limited to, system logs, directory listings, electronic mail files, screen prints of error messages, and database activity logs.
4. **Take notes.** Record all relevant information, including things you observed, actions you took, dates and times, etc. It is best to log your activities as they occur.
5. **Changing account passwords.** All system accounts that were involved with the incident may require new passwords as determined by the Information Security Officer. Choose a password in accordance with the [password requirements](#) and change it every ninety (90) days.
6. **ITS will determine the correct course of action.** The appropriateness of each course of action varies with the severity of the incident (amount of damage, legal implications, cost of recovery, etc).

Other Steps A Systems Administrator May Take

1. **Change the status of accounts, if necessary.** In the event that a system administrator detects a problem with a system, or questionable user activity on a system, a quick way to stop the unwanted activity is to "close" an account, by restricting logins to it. This results in the account owner having to contact an administrator in order to remove the login restriction. This is *not* deleting the account, but is merely making the account temporarily unusable.
2. **Stop rogue service(s), if necessary.** In the event that a system compromise or denial-of-service attack is underway, and you are unable to stop or kill the service(s), you may need to disconnect the machine from the network. Examples of this type of attack is a "ping sweep" which occurs when one machine on the network sends other machines Internet Control Messages Protocol (ICMP) requests until the network exceeds capacity causing degradation and/or traffic being blocked.
3. **Review your backup policies.** If you believe your data and/or operating system has been compromised, you must ensure that a backup is available for restoration. If your next backup *could* overwrite an undamaged backup, take *immediate* steps to prevent that occurrence. If your disaster recovery policy includes multiple levels of backup, and you are uncertain how long the system has been compromised, you must determine which backup version to restore to. Until that time, do not allow any backups to be overwritten. It is recommended that users regularly back up important data (e.g., student/patient/employee information, data related to Institutional operations, vital mission data, etc.) to a floppy disk or to a drive on the server (see your Department Administrator for Departmental I.T. Representative for access restrictions) at least once a week (or more often for more critical data.)

If you have questions about incident procedures, contact its@ttuhsc.edu.

1.4.8 INTERNET AND INTRANET CONNECTIVITY

The CIO is responsible for providing Internet connectivity for the TTUHSC network. Regional campus LANs, or any other supported or non-supported LAN connected to the TTUHSC network, may not connect to any other Internet service provider without written approval of the TTUHSC Information Security Officer (ISO) and Managing Director of Technology Services.

The CIO or their designee must authorize all network connections between the TTUHSC network and external government agencies or affiliated teaching hospitals. These connections will be controlled and monitored by a firewall or other security device under the administrative control of the Information Security Officer and his/her staff.

Access to the Internet and intranet are for Institutional purposes. Please refer to policy [1.4.1 Acceptable Use](#) for additional information.

1.4.9 INTRUSION DETECTION

The Information Technology Security Group shall monitor and audit intrusion detection logs as part of their daily job functions. Intrusion detection logs are maintained for a minimum period of two weeks. Anomalies will be investigated and appropriate measures will be taken in the event of an actual threat in accordance with the incident management procedures outlined in [Policy 1.4.7, Incident Management](#). Compliance with this policy is the responsibility of the Information Security Officer.

Various tools provide the ability to block malicious programs on our email servers, file servers and other computers on our network.

1.4.10 NETWORK ACCESS

Local Area Networks

Supported LANs are those designed, installed, and operated by the Enterprise Network team. Devices such as computers, printers, scanners, storage devices and arrays, and video-conferencing systems may be connected to a network outlet within a supported LAN with the approval of the campus RSC.

The following may not be connected to an outlet within the TTUHSC network without prior written authorization of the CIO or their designee:

- Proxy servers and firewalls
- Systems or devices providing Virtual Private Networking (VPN) capability to the Internet
- Wireless [access points](#) or other wireless networking equipment (Refer to [Wireless Access](#))
- Hubs/switches/routers/bridges.
- Systems or devices containing a network adapter operating in promiscuous mode where a node on a network accepts all packets, regardless of their destination address
- Systems performing Network Address Translation (NAT)

- Systems operating Domain Naming System (DNS), Windows Internet Naming System (WINS), or Dynamic Host Configuration Protocol (DHCP) services.
- Windows Domain Controllers

TTUHSC Domain

All TTUHSC owned PCs and servers attached to the TTUHSC network must be members of the TTUHSC domain and be defined in the appropriate Active Directory Organization Unit (OU)

Modem Connections

All modem connections must be approved by the CIO or their designee, and routed through a modem pool or network device which utilizes an I.T. approved authentication system.

The connection of a device to the TTUHSC network that is accessible directly from the Internet, without going through the TTUHSC firewall or an I.T. managed modem pool, is a security risk. Typically, this is a modem device connected to a desktop computer or server on the TTUHSC network which is set to automatically answer incoming calls for connections to outside systems. Incoming connections to modems are not allowed without CIO approval.

Remote Access Policy and Procedures

Remote access to the TTUHSC network provides users with the convenience of accessing the Internet, their office computer, or information on network file shares to which they have access. Along with this convenience, comes the need for appropriate security controls to ensure that data transmitted is secure. Additionally, the network must be protected from illicit use; and to ensure that viruses, malware, and other malicious code are not allowed to propagate across the network.

Scope

This policy applies to all remote devices connected to the TTUHSC network infrastructure through Internet access or direct dialup connections.

Policy

State and federal legislation requires TTUHSC to provide protection for sensitive data such as patient information and student financial data. Therefore, TTUHSC personnel must use a secure mechanism for accessing the TTUHSC network infrastructure remotely. Additional information on remote access can be found at www.ITsolutions.ttuhs.edu.

All users who connect remotely to the TTUHSC network must install an anti-virus software on each computer. This anti-virus software must be updated regularly with new anti-virus signatures. TTUHSC provides free McAfee Virus Scan licenses for home use by faculty, staff, and students. This software can be downloaded at <https://www.ttuhs.edu/IT/security/mcafee/>.

VPN

Any user accessing the TTUHSC network through an Internet connection (Satellite or [cable](#) Internet connections) must connect using a Virtual Private Network connection (VPN).

Account Administration

VPN accounts are available at no cost for current faculty, staff, and students of TTUHSC. VPN accounts can be requested at www.ITsolutions.ttuhs.edu. An email response will usually be returned with account information and setup instructions within 1 business day.

When a VPN account holder (employee or student) leaves TTUHSC, the account will be disabled as soon as Information Technology is notified of the termination date. VPN accounts will be set to automatically expire 12 months from the date the account is created or renewed. At least one week before an account expires, an email will be sent to the account holder reminding him/her to renew the account. The renewal request can be filled out at www.ITsolutions.ttuhs.edu.

Client Connection Setup

VPN services from connections outside the TTUHSC network are supported, provided that VPN services are in compliance with the Internet Service Provider's policies.

Security

All Institutional security policies are applicable to remote access users. Security controls in place include appropriate authentication and Intrusion Prevention Services (IPS). Monitoring and auditing will be conducted on the remote access connections in the event of unusual network activity. Information Technology will disable a dial-up or VPN account, based on recommendations from the I.T. Security Team, if network activity from any remote access computer is disrupting computing services on the TTUHSC network.

TTUHSC Software Requirements

All systems connected to the TTUHSC network must have approved anti-virus software ([I.T. Policy 1.4.22, Viruses and other Malicious Code](#)) installed and operational before the system is connected to the network. This software must be configured to receive regular virus signature updates from the anti-virus servers administered by the TTUHSC Information Security Officer and his/her staff.

1.4.11 NETWORK CONFIGURATION

This policy describes the requirements and constraints for attaching a computer, system, or network devices, or videoconferencing system to the TTUHSC network. The intent of this policy is to ensure all connections to the TTUHSC network are maintained at appropriate levels of security and interoperability, while at the same time not impeding the ability of TTUHSC faculty, staff, and students to perform their work.

Responsibilities

The Chief Information Officer (CIO) is the central authority for all network issues. The CIO may appoint and/or delegate management of certain aspects of network administration as deemed necessary.

TTUHSC regional campuses administer local area networks (LAN), under direction of the CIO and the Managing Director of Technology Services. Each regional campus or location must designate a [Regional Site Coordinator \(RSC\)](#) to serve as the administrator of all LANs at that campus. The RSC is the contact person for all connectivity issues between the regional campus LANs and the TTUHSC wide area network (WAN).

The Managing Director of Technology Services is the main point of contact with Facilities Planning and Construction and Physical Plant at all campuses for all new construction and major renovation projects involving computing systems. Minor renovations will be handled at the local level.

Wide Area Network Connectivity and Routing

All routers within the TTUHSC WAN will be selected, operated, and maintained by personnel designated by the CIO. Subnet IP routing on the TTUHSC WAN will be performed in accordance with delegated IP address space. Routing of private IP address space (as defined by the [Internet Engineering Task Force Request For Comments document #1918 - Address Allocation For Private Internets](#)) across the TTUHSC WAN must be approved by the CIO or their designee.

Firewall Access Standard

All internal TTUHSC computers are protected from outside network access by a [firewall](#). All incoming network requests not known and defined are denied and are not passed through to the internal campus network. This section describes the procedures to allow special access through the firewall to employees and third parties/vendors in instances where certain services and /or applications are required to maintain workflow and provide services.

Standard

Approval for outside network access to TTUHSC computing resources will be based on the following criteria:

- The connection is required for TTUHSC business,
- The connection does not represent an unnecessary security risk to TTUHSC,
- The connection does not use an insecure protocol where a more secure alternative exists, and
- The connection does not involve unnecessary replication of functionality

When the connection has been approved by the CIO, firewall access will be granted when the following have been completed:

- The machine is properly registered with Information Technology by filling out the Special Firewall Access Request Form at <http://www.ttuhs.edu/it/forms/firewallreq.aspx> and sending it to the [I.T. Solutions Center](#).
- The target machine passes a vulnerability assessment performed by I.T. Security (ITS). This assessment consists of remotely scanning the target machine for common problems that could result in a security risk.
- The target machine has a reserved IP address.

Registration ensures that the target machine has an administrator known to Information Technology. The administrator will perform the necessary tasks to keep the system up to date and in a secure state, with the assistance from the Information Technology Security Group. Registration will be renewed once a year. Renewal notices will be sent via email by the ITS.

The ITS will perform routine security scans on machines registered for special access.

Procedures

The firewall access form should be submitted through the web to itsolutions@ttuhs.edu. Depending on the request, it may take up to two business days for the request to be completed. If the request is considered urgent, and the two-day timeline is not sufficient, please state that the request is Urgent. Include in the email message the reasons why the request is time critical.

Request for changes to the firewall must come from the administrator of the target machine. Requests received from anyone else will be forwarded to the machine's administrator for approval.

All requests will be sent to the Regional Site Coordinator (RSC) at the campus where the machine resides. Once the RSC has checked to make sure the machine has a reserved IP address, the request will be forwarded to the Information Technology Security Group for final approval by the Information Security Officer. Once approved, the Information Technology Security Group will make the necessary changes to the firewall. The RSC may require that network configuration of the destination computer be modified prior to approving access.

IP Address Allocation Standards And Procedure

IP Addressing

All address delegation with the regional campuses and any supported LANs will be coordinated between the CIO or their designee and with the appropriate RSC. The RSC will be responsible for administration and registration of all IP addresses and sub-networks within the delegated address range(s), according to the standards and guidelines approved by the CIO. All [hosts](#) in the TTUHSC domain must obtain a valid IP address from the RSC. No host on the intranet

should broadcast dynamic routing information except specially configured gateway or router devices.

To ensure efficient IP address utilization, TTUHSC will allocate their assigned IP addresses to reflect the requirements of each building location, wiring closet, or network service. This ensures compliance with the American Registry for Internet Numbers (ARIN) requirements for utilization of public IP address space.

For regional IP addressing strategy, RSC's should refer to the [IP Address Allocation Strategy](#).

Reserved IP Address Standards

Reserved IP addresses are available to the following hosts:

- Server systems that provide file sharing, printer sharing, or other application services to multiple client systems
- Printers with a direct network attachment
- Hosts with a directly attached printer, where print jobs will be accepted from client systems on the network
- Hosts providing services or resources to clients outside the TTUHSC network. Refer to the [Firewall Access Standards](#) for details on requesting this type of access.

All other hosts will use dynamic addresses, allocated by Dynamic Host Configuration Protocol (DHCP) services at each regional campus. Reserved address requests for hosts that do not correspond with the above list must be approved by the appropriate Regional Site Coordinator.

Refer to the [Server Hardening](#) Section for additional requirements that must be met before a server can be assigned a reserved IP address.

Reserved IP Address Allocation Procedures

All reserved IP addresses must be properly authorized and recorded before they are issued. The following outlines the procedure for requesting and allocating reserved IP addresses:

1. Complete the [Reserved IP Address Request form](#) and send to the Regional Site Coordinators at the respective campuses.
2. Upon receipt, the network technician creates a work order, and verifies the attached information is complete.
3. Using the TTUHSC IP Address Management application, the host is assigned to the correct VLAN and subnet. The next available address is selected, and the information provided by the requestor is entered into the system.
4. The assigned IP address, hostname, and hardware address are entered into the DHCP server(s).
5. If requested, Domain Name Service/System (DNS) alias entries are entered into the DNS configuration file to translate domain names into numeric IP addresses.
6. The assigned IP address is sent to the requestor via email.

7. The technician updates and closes the work order.

1.4.12 PASSWORD/AUTHENTICATION

Never share your password with anyone.

In accordance with [Texas Administrative Code § 202.75](#), all TTUHSC computing systems shall require a login authentication process, whereby each user is identified and authenticated through their unique USER ID and/or account name. Access to the network and to applications is based on individual roles and determination of user access levels is the responsibility of the owners of the information or applications being accessed.

Texas Tech's primary authentication is through an account management system known as eRaider, which allows users to access the information resources available at the Health Sciences Center. Passwords for eRaider accounts follow industry best practices and must meet the following requirements:

- 8 - 15 alphanumeric characters,
- Contain upper & lower case characters,
- Contain a number,
- NOT contain a number as the first or last character,
- NOT contain any word found in a dictionary, and
- May contain punctuation marks.

Passwords must be reset every 90 days.

System Identification/Logon Banner

Any TTUHSC computing system that prompts the user for a login should require an unauthorized access warning banner be displayed. The [unauthorized access warning banner](#) must inform the user of the restrictions imposed on the system before access is attempted, thereby giving the user the opportunity to avoid violating any access restrictions. The Unauthorized Access Warning Banner must be prominently displayed each time a user attempts to access a server system, network terminal, and/or a restricted/secured [web site](#) and/or [web page](#), specifically before the user can begin the login authentication process.

The Unauthorized Access Warning Banner will be made part of the web site and/or web page preceding a restricted/secured web site and/or web page and must be displayed before a user enters the secured web site and/or web page. The user must also be made to acknowledge the warning either in the form of an icon or button stating "OK" or "I Accept" before they can proceed.

Unauthorized Access Warning Banner Text

The following is the text for the Unauthorized Access Warning Banner:

WARNING!

USE OF THIS SYSTEM IS RESTRICTED TO AUTHORIZED USERS ONLY AND SHALL BE USED IN ACCORDANCE WITH THE ACCEPTABLE USE POLICY. THIS SYSTEM MAY BE SUBJECT TO MONITORING BY THE INFORMATION TECHNOLOGY DIVISION. UNAUTHORIZED ACCESS IS A VIOLATION OF APPLICABLE TTUHSC, STATE, AND FEDERAL LAWS AND REGULATIONS AND WILL BE SUBJECT TO CRIMINAL PROSECUTION.

1.4.13 ASSET MANAGEMENT

Information resource assets consist of hardware, software, and information. Software and Hardware assets are to be controlled according to requirements of [O.P. 63.10, Property Management](#). Appropriate disposal processes are in place by General Services. Departments are responsible for software and data files on computing devices and equipment before they are transferred or surplus unless the software license is transferable. In the event that the computing device contains any confidential information in electronic media, the department is responsible to ensure that all electronic media is destroyed prior to being transferred or surplus.

1.4.14 PORTABLE COMPUTING

TTUHSC has seen a significant increase in the use of the Portable Computing Devices (laptops, Personal Digital Assistant's (PDA), smart phones, USB drives, and USB flash drives) at the Institution. This policy is intended to provide guidance for Portable Computing Device utilization.

Security Guidelines

Portable Computing Devices are inherently at risk for theft and security vulnerability. In cases where there is a justifiable business need or requirement for confidential information, such as patient information, confidential student information, grades, etc., to be stored or transferred to a Portable Computing Device appropriate security measures must be implemented as listed below.

Security Policy

- Confidential information shall not be stored, downloaded, or leave the Institution unless there is a need to access this information away from the Institution. Authorization will need to be obtained by each individual from the information owner. Information owner responsibilities, definition, and more information can be found in [Policy 1.1, I.T. Resource Management and Responsibilities](#).
- Confidential information shall not be shared with others who do not have a job-related need for this information.
- Confidential information should not be copied to or stored on a portable computing device, removable media, or a non-state owned computing device that is not encrypted.

- The Portable Computing Device must be password protected using the security feature provided on the Portable Computing Device and there should be no sharing of the password.
- Removable media such as memory cards must not be used to store confidential information.
- A Desktop PC that is used for synching must have approved antiviral software installed, and require user log on.
- Whenever there is no longer a job related need to access or store this confidential information, it must be deleted.

1.4.15 PRIVACY

Rights to personal privacy, while using Institutional I.T. resources, will be maintained in accordance with federal and state statutes. Furthermore, user activity may be monitored pursuant to [Policy 1.4.16, Monitoring of I.T. Assets](#) of this policy. For further information, please refer to the links in the [Federal](#) and [State](#) statutes section.

In addition, the safeguarding of certain financial information (including, but not limited to information used in connection with the awarding and issuance of student loans) that is covered by the [Gramm-Leach-Bliley Act of 1999, 15 U.S.C. 6801](#), et seq., implemented by [16 CFR Part 314](#), will be governed by the TTUHSC Information Security Plan for Financial Information and [TTUHSC OP 56.01 – Use of Information Technology Resources](#).

[TTUHSC O.P. 56.04](#) states that anyone who has access to confidential information will take reasonable and necessary steps to maintain the confidentiality and privacy of such information.

As a key provider of services and technology in the healthcare industry, TTUHSC has implemented programs to address the transaction standards, and the privacy and security implications of the rules set forth by the [Health Insurance Portability and Accountability Act \(HIPAA\) of 1996](#). More resources on HIPAA can be found at <http://www.ttuhs.edu/hipaa/>.

1.4.16 MONITORING OF I.T. ASSETS

As a public institution, all TTUHSC computers, [videoconferencing systems](#), and network activity are subject to ongoing and unannounced security audits. The inappropriate use of the systems and/or networks that violate Institutional policies or local, state and federal laws (i.e., copyright violations, pornography) will be investigated and reported. The CIO or their designee will authorize these investigations and the appropriate authorities will be notified. The Information Technology Security Team will be responsible for conducting these audits as necessary.

TTUHSC has the right to disclose the contents of electronic files, as required by legal, audit, or legitimate State, Local, Federal and/or Institutional purposes.

1.4.17 SECURITY AWARENESS AND TRAINING

TTUHSC will use the "New Employee Orientation" to initiate security and copyright awareness and educate new employees about TTUHSC I.T. policies. Annual Security Awareness Training will be required for all faculty and staff who access the TTUHSC network. The ISO will be responsible for assuring that the appropriate training is provided and utilized by all network users.

The Information Security Officer, in collaboration with the I.T. Security Council, will ensure additional security awareness will be provided through ongoing web announcements and other media formats.

1.4.18 SERVER HARDENING

Standard/Procedure

A server cannot be connected to the TTUHSC network until it is in a TTUHSC I.T. approved secure state. Prior to connecting the server to the network, the following must be performed:

- Complete a Server Registration Form (<http://www.ttuhs.edu/it/forms/serverregistration.aspx>)
- Install the operating system from an I.T. approved source which includes proper licenses,
- Receive a reserved IP address from the appropriate regional campus network administrator,
- Remove all unnecessary software, system services, and drivers,
- Set appropriate security parameters, file protections, and enable audit logging,
- Disable or change the password of default accounts, and
- Complete a Server Registration Form (<http://www.ttuhs.edu/it/forms/serverregistration.aspx>) and submit it to its@ttuhs.edu.

Before connecting to the network

- Install I.T. approved anti-virus software, and

Immediately after connection to the network, the following must be completed:

- Apply the latest vendor supplied patches, which have been tested for compatibility with the production environment.

Note: For more detailed information and procedures based on specific operating system, please refer to Guidelines For Operating Systems Security at <http://www.ttuhs.edu/it/policy/ossecurity.aspx>.

All servers are required to be submitted to a vulnerability assessment performed by TTUHSC Information Technology Security group (ITS) prior to use.

In the event that a vulnerability or a combination of vulnerabilities are discovered that constitute an unacceptable level of risk as deemed by TTUHSC ITS, the server administrator is responsible

for ensuring they are addressed. Any such risk must be addressed prior to production use. Further scanning may be required.

TTUHSC ITS will monitor security issues, both internal and external to TTUHSC, and will monitor the release of security patches on behalf of TTUHSC. After the server administrator is notified by the ITS, patches must be implemented within a specified timeframe determined by the security level of the patch, or the risk level of the vulnerability. ITS will routinely monitor to ensure the system(s) are in compliance. Failure to comply with these guidelines can result in the server(s) being removed from the network.

TTUHSC I.T. will perform due diligence in testing security patches before release when practical.

1.4.19 AUTHORIZED SOFTWARE

Installation of any software must have a justifiable business purpose and must be properly licensed. Standard recommended software can be found at www.ITsolutions.ttuhs.edu/support.aspx. Software that is Institutionally-required (e.g., McAfee VirusScan) must not be removed. Each system should also be set to automatically receive Microsoft Updates. The CIO, or designee, reserves the right to remove any software on computers that poses a threat to TTUHSC computers or to the operation of the network.

1.4.20 APPLICATION SYSTEM DEVELOPMENT, ACQUISITION, AND LIFECYCLE

The central Data Center at TTUHSC employs a three-tiered architecture that consists of separate testing, staging, and production servers that isolates the testing environment from production environment. All server or web-based applications residing in the central Data Center must be hosted in this type of environment to ensure separation of test and production code/data. PHI data and the services that manage that data must reside on servers located in the central data center with limited access and additional security controls. Within this section, applications are defined as programs, software, systems, or web pages that are available to and interact with multiple users. These applications and associated data usually have a medium to high risk associated with them, as defined in [Policy 1.1, I.T. Resource Management and Responsibilities](#). (See also [TAC 202.72](#))

Access to the production environment must be strictly controlled. Web development and quality assurance practices are described in [Policy 9.4, Change Management](#), Procedures for Official TTUHSC Web Pages/Sites. The quality assurance process for developing, maintaining and changing applications at TTUHSC is described in this section.

Developing Applications/Systems/Web Pages

All applications/systems, acquisition, development, and maintenance will be required to undergo a security audit before being put into production and must follow [Policy 9.5, Coding Standards, Security, and Audit Controls](#).

Migrating Applications/Systems/Web Pages From Test To Production

Within the Information Technology Division at all campuses, all developers must adhere to the following quality assurance procedures:

- All developers and the requesting department are required to thoroughly review and test the application/system/web pages in the testing environment prior to it being moved to production. In many cases, this will require the development of testing documentation that includes test cases and scenarios. If the requesting department is not the owner of the application/system/data, then the application/system/data owner must also be involved in the review and testing. This testing must be completed before the security code review can be conducted.
- All applications/systems/web pages are required to undergo a security code review by Information Services prior to production implementation. A work order for a code review should be submitted via [STARS](#). IS staff will perform a security code review for the project prior to it being moved into production. When requesting a security code review, please allow for adequate time (24-72 hours). The security code review will include the utilization of third party software that is specifically designed to identify vulnerabilities.
- Once the security code review is completed and all vulnerabilities have been addressed, the requesting department must request that the application/system/web pages be moved into production. The request to move to production will be approved by the Associate Vice President for Information Services or the Managing Director of Information Services. If the requesting department is not the owner of the application/system/data, then the application/system/data owner must also approve the move to production.
- Designated personnel will migrate the application/system/web page and any applicable data sources from test into production using a documented process. This process should include:
 - Implementation procedures and requirements, and
 - Making and documenting any changes to IIS, access privileges, etc. necessary to the proper functioning of the application.
- For applications/systems/web pages residing in the central Data Center, Information Services Project Leaders migrate the code and Information Services DBA's migrate any applicable databases into production. The migration of code from the test environment to the production environment is handled by a process developed in-house called the HSC [Application Publisher](#). The HSC [Application Publisher](#) is a program designed to control the publishing of applications to the production environment. The application allows users to publish new versions of applications from a specified share to the production environment while giving the user the ability to save a copy of the version they are replacing. The application also does not allow any user to publish to production unless their code has undergone an initial security code review.
- After it is moved into production, the developer and the requesting department are required to do a final review and test of the application/system/web page developed. Once this is completed, the requesting department and the application/data owner are also required to submit a final approval for the project to the developer.

Outside of the Information Technology Division at all campuses, all developers should adhere to the same quality assurance procedures listed above. However, all applications/systems/web pages are required to undergo a:

- Security code review by Information Services prior to production implementation. A work order for a code review must be submitted via [STARS](#) IS staff will perform a security code review for the project prior to it being moved into production. When requesting a security code review, please allow for adequate time (24-72 hours). The security code review will include the utilization of third party software that is specifically designed to identify vulnerabilities.
- Once the security code review is completed and all vulnerabilities have been addressed, the requesting department must request that the application/system/web page be moved into production. The request to move to production will be approved by the Associate Vice President for Information Services or the Managing Director of Information Services. If the requesting department is not the owner of the application/system/data, then the application/system/data owner must also approve the move to production.

All applications/systems/web pages residing on servers outside of the central Data Center will be hosted using a three tiered architecture and must follow the below approval process. The Architecture must consist of separate testing, staging, and production servers that isolate the testing environment from production environment and utilizes the quality assurance procedures listed above for the Information Technology Division.

All coding will be consistent with the practices outlined in [Policy 9.5, Information Services Coding Standards, Security, and Audit Controls](#).

Submitting A Project Request For Information Services Resources

- A project request must be submitted to Information Services for:
 - Any modification or enhancement to an existing web site, web application, or other system,
 - The development of new web sites, web applications, or systems,
 - The implementation or upgrading of database or storage systems,
 - The implementation or upgrading of acquired software or systems,
 - The development or modification of [e-Commerce](#) applications,
 - Security reviews for developed or newly acquired web sites, applications, or systems. All requests for security reviews for new software, applications, or systems should be made at the beginning of the procurement process to allow sufficient time to conduct the security review before procurement, and
 - An appropriate Project Management review to be completed.

All project requests are reviewed on a bi-weekly basis. The purpose of this review is to determine whether resources exist to accomplish the objectives of the request and to prioritize approved requests. Before any project can be scheduled and resources allocated, it must be approved by the Associate Vice President for Information Services or the Managing Director of

Information Services **and** the applicable Campus I.T. Director prior to any allocation of resources.

Also, if a request is submitted and the request was not made by the application/data owner, then the application/data owner must approve the request prior to any work starting on the project.

Projects are requested by submitting a work order via [STARS](#).

- Once a request is received, it is reviewed for both resource availability and Project Management needs. If the resources are available and the request is approved, it is assigned to an Information Services staff member(s).
- The assigned staff member(s) will:
 - Contact the requestor for additional information and further define the request,
 - Gather the scope requirements of the request,
 - Prepare the necessary project documentation
 - Obtain agreement on the scope and requirements of the project and obtain sign-off to begin work,
 - Begin work on the maintenance or application development project in the test environment,
 - Work with the requestor so that the maintenance change or developed application can be reviewed and tested, and
 - Make any changes or corrections discovered during the review and testing,
 - Request a security code review and make any necessary adjustments
 - Conduct a final round of review and testing,
 - Obtain sign-off from the appropriate parties for production implementation,
 - Wrap up the project.

1.4.21 VENDOR ACCESS

Vendors' physical access to the central Data Center will require the appropriate approval and authorization by the CIO or the Managing Director of Technology Services. Logs will be maintained on all vendor access to the central Data Center facilities and vendors must execute a Business Associate Agreement with the Institution prior to accessing the TTUHSC network to ensure that any confidential information intentionally or unintentionally accessed is properly protected. Vendor access is for a limited time only.

1.4.22 VIRUSES AND OTHER MALICIOUS CODE

The purpose of this policy is:

- To establish procedures that define the responsibilities for reducing the threat of computer viruses to TTUHSC computers and networks
- To establish responsibility for overseeing computer virus prevention activities within TTUHSC, and to establish a reporting mechanism to ensure all appropriate personnel are contacted in case of a computer virus incident

- To promote awareness of the threat posed by computer viruses to TTUHSC students, faculty, staff, and to ensure that virus protection software and procedures are properly implemented and utilized on a regular basis

Due to the collaborative nature and sensitivity of the work performed at TTUHSC, all Institutional computers must have the institutionally provided antivirus software installed. Users' continued access to the TTUHSC network is contingent on the installation of institutionally provided antivirus software on all TTUHSC-owned computers. This virus protection software must not be disabled, bypassed, or modified in any way.

Specific Restrictions

TTUHSC expressly prohibits:

- Development of any form of computer virus with the intent to distribute through the TTUHSC network or beyond
- Intentional distribution of a virus, regardless of type (nuisance or destructive)
- Intentional creation of false alarms using hoax virus messages

Specific Responsibilities and Guidelines for Virus Prevention

Students, Faculty, and Staff should:

- Understand the risks associated with viruses and preventative measures that can be reasonably deployed.
- Be aware of and follow the procedures outlined in TTUHSC I.T. announcements (web page or email), which will be used to communicate warnings of potential computer virus threats.
- Treat nuisance viruses with the same urgency as destructive viruses. Write down the name of the virus, if provided by the virus detection software.
- Write down any recent unusual computer activities (for instance, unexpected disk access, error messages, or screen displays) and, if possible, include when these activities were first noticed.
- Contact the [Information Technology Solutions Center](#) when a computer virus is suspected and/or detected.
- Never boot directly from external devices or media until they have been scanned for viruses. By default, the Institutional antivirus program is configured to automatically scan all devices upon use. (This is completely done in the background without any visible disruption to the user.)
- Ensure files received from external sources are clean of viruses prior to use or distribution and never use or introduce non-licensed software on any TTUHSC [computing device](#).
- Back up critical data (e.g., student/patient/employee information, data related to Institutional operations, vital mission data, etc.) to a floppy disk or to a drive on the server (see your Department Administrator or Departmental I.T. Representative for access restrictions) at least once a week (or more often for more critical data.)

[Computer Security Analyst \(CSA\)](#) is responsible for:

- Isolating the infected computer(s) from the TTUHSC network as soon as possible. Reasonable attempts should be made to notify the primary user or the system administrator before disconnecting from the network. Depending on the nature of the virus, this may not be possible and the [I.T. Solutions Center](#) should be contacted prior to disconnecting a computer from the network. The Solutions Center will coordinate the ITS and networking to minimize any potential risks.
- Identifying and isolating the suspected virus or worm-related file and processes. Do not power off or reboot computers that may be infected. There are some viruses that will destroy disk data if the computer is power-cycled or rebooted. Also, rebooting a computer could destroy needed information or evidence.
- Attempt to halt and/or remove all suspicious processes from the computer. In the case of a worm attack, it may be necessary to keep the computer(s) isolated from the network until all TTUHSC computers have been inoculated and/or the other Internet sites have been cleaned and inoculated.
- Implement fixes and/or patches to inoculate the computer(s) against further attack.
- Notify the ITS prior to bringing the computers back into full operation mode. The users should also be notified the computers are returning to a fully operational state.

Information Technology Security (ITS)'s responsibilities include:

- Overseeing computer virus protection activities within TTUHSC which include the desktops and servers, Internet mail gateway, and Exchange Servers. This is done in coordination with the CSAs.
- Staying current with the latest virus exploits and maintaining attachment filtering lists through the mail servers.
- Evaluating, recommending, and maintaining virus protection software and/or tools for use on TTUHSC PCs, servers, and laptops.
- Coordinating any training on virus control required for CSAs and TTUHSC personnel in general.
- Investigating every report of an apparent computer virus infection, and making every reasonable effort to determine the source of the infection. The Information Security Officer will keep all affected personnel advised of the investigation.
- Monitoring compliance of virus protection policies.

The CSA and ITS are jointly responsible for:

- Verifying the existence and identifying the type of virus on the user system.
- Coordinating with the anti-virus vendor or other sources on disinfection methods.
- Documenting any recent unusual computer activities (for instance, unexpected disk access, error messages, or screen displays) and, if possible, including when these activities were first noticed.
- Ensuring that the appropriate data for the monthly [Department of Information Resources virus report](#) is received by the Information Security Officer no later than the second business day of each month.

Information Technology PC Support/System Support (all campuses) should take the following steps:

- Ensure that virus protection software is installed on every desktop, server, and laptop computer acquired by TTUHSC before they are made available for use by TTUHSC students, staff, or faculty,
- Ensure that the virus protection software has loaded a 'terminate and stay resident' (TSR) program or service/daemon to constantly monitor for viruses to prevent introduction to the network,
- Inform the ITS/CSA of new anti-virus installs. This procedure is to make sure the desktop, server, or laptop can communicate with the anti-virus management server to receive updates,
- Upon receipt of a notice of a possible virus, clarify the symptoms with the user,
- Verify if there is a virus and if so, report the incident to the ITS/CSA, and
- In the event the virus cannot be removed from the infected computer, the ITS/CSA will contact PC Support or System Support to rebuild the computer.

1.4.23 WIRELESS ACCESS

To ensure proper administration and security of the network, it is important for the development of wireless networking capabilities to be controlled and coordinated.

This document outlines the policies for the implementation of wireless networking technology at TTUHSC. See also [Policy 1.4.14 - Portable Computing](#).

Scope

This policy applies to all wireless network devices connected to the TTUHSC network infrastructure, or wireless devices owned by TTUHSC, or operated in TTUHSC facilities.

Policy

All TTUHSC faculty, staff, and students should be aware that wireless network connections are inherently less secure than wired connections. State and federal legislation requires TTUHSC to provide protection for sensitive data such as patient information and student financial data. Therefore, TTUHSC personnel are advised against using wireless technology to transmit this type of information.

Information Technology will extend the TTUHSC network to provide wireless service to any area based on the application need and demand and subject to the availability of resources. Wireless networks are not a replacement, but a supplement to the existing wired network.

The Chief Information Officer (CIO) or designee, in concurrence with the Regional Site Coordinator (RSC) at the respective campus, must approve the installation and use of wireless access points connected to the TTUHSC network.

These access points and wireless devices must have the manufacturer's default SSID changed. These access points and devices will be audited and monitored on a regular basis. Information Technology reserves the right to remove any unauthorized or misconfigured wireless device from the network immediately without prior notice.

Wireless networks and services are subject to the same rules and policies that govern other electronic communications services at TTUHSC. (See [Acceptable Use](#) and [Portable Computing](#)). Disruption of authorized communications or unauthorized interception of wireless communication is a violation of policy.

Equipment

TTUHSC will implement wireless equipment that follows the [IEEE 802.11](#) standards. Wireless equipment standards will be reviewed and amended as wireless standards change, and as products are introduced that improve the security and reliability of the wireless network.

Security

Access to the wireless network will be limited to individuals [authorized](#) to use the Institutional network and Internet resources. All wireless network users must authenticate his/her identity to an authentication server managed by Information Technology before access to the rest of the TTUHSC network is permitted. Anonymous users will not be allowed to access the wireless network.

Responsibilities

Information Technology

- Develop, maintain, and update wireless communications policies and wireless networking standards.
- Approve standards for wireless network hardware and software used by TTUHSC.
- Approve, design, and install wireless network equipment for all TTUHSC locations.
- Inform wireless users of security and privacy policies and procedures related to the use of wireless communications.
- Monitor security of all wireless networks within the TTUHSC network to prevent unauthorized access to the TTUHSC network.
- Monitor the development of wireless network technology, evaluating wireless network technology enhancements and, as appropriate, incorporating new wireless network technology with the TTUHSC network infrastructure.

Department Administrators

- Ensure departmental compliance with all applicable TTUHSC policies pertaining to the installation and use of the wireless network.
- Inform wireless users of security and privacy policies and procedures related to the use of wireless communications.

- Notify Information Technology when modifications to the network are needed.

1.4.24 VULNERABILITY ASSESSMENT

Vulnerability applies to all institutional computing devices. Vulnerability assessments will be conducted periodically to test security measures currently in place. When vulnerabilities are detected that constitute an unacceptable level of risk as deemed by TTUHSC ITS, the server administrator will be notified of the vulnerabilities. The server administrator is responsible for ensuring that the risk is mitigated in a timely manner.

2. INSTITUTIONAL VIDEOCONFERENCING SYSTEMS

The TTUHSC Information Technology (I.T.) Division operates, maintains, schedules, and supports Institutional videoconferencing systems installed in classrooms, conference rooms, auditoriums, teaching studios, telemedicine facilities, network control centers, and similar facilities at TTUHSC and affiliated locations. Collectively, these facilities and systems are known as the TechLink Video Network. To preserve the value of this technology as an educational, healthcare, and communications medium, it is necessary to set standards for hardware and software acquisition, acceptable use, security, configuration management, user training, resource reservation (scheduling), upgrade, and replacement concerning TTUHSC Institutional videoconferencing systems.

This policy applies to all videoconferencing equipment, systems, software, and services connected to the TTUHSC network or operated in TTUHSC facilities. Included are the Event Management System (EMS) for scheduling TechLink services, TechLink Multi-media Teaching Podium systems, fixed and mobile videoconferencing systems, telemedicine videoconferencing systems, document cameras, video cameras, microphones, monitors, projectors, smart boards, PCs, laptop PCs, studio facilities, audio and videoconferencing bridges, video codecs, content capture and streaming devices, satellite earth station facilities, and all associated systems infrastructure.

Responsibilities

The Telecommunication Services Department acquires, operates, maintains, manages and schedules Institutional videoconferencing systems at TTUHSC; with strategic oversight and operational direction from the Chief Information Officer (CIO) or designee. The Senior Director of Telecommunication Services is the designated point of contact for all matters involving videoconferencing at TTUHSC.

Acceptable Use

Institutional videoconferencing systems are multiple user facilities throughout the TTUHSC System. Their use is based on adherence to standards of acceptable use and respect for the needs of other users and user groups. Additionally, these systems are intended for official TTUHSC and state business only, and certain requests for their use may require approval from the TTUHSC General Counsel. Institutional videoconferencing equipment, systems, software, and

services are subject to the same policies and rules that govern other electronic communications at TTUHSC. (See also [Copyright](#), [Disciplinary Process](#), [Acceptable Use](#), and [Security](#)).

Technical Standards

TTUHSC will implement videoconferencing systems and services which adhere to industry best practices; the Advanced Television Standards Committee (ATSC) and National Television Standards Committee (NTSC) protocols; and the H.320 and H.323 families of communication standards. This policy will be reviewed and amended as best practices and communication standards evolve; and as products and services emerge that improve videoconferencing quality and reliability. Only videoconferencing hardware, software, and services approved by the CIO or designee may be installed on Institutional video conferencing systems. (See also [I.T. Procurement Review](#) and the section below on Connectivity).

Connectivity

Only videoconferencing hardware and software approved by the CIO or designee may be connected to the TTUHSC network. (See also [I.T. Procurement Review](#), [Network Access](#), [Security](#), and the section above on Technical Standards). As an added measure, departmental and personal media storage devices such as CDs, DVDs, PCs, laptop PCs, and thumb drives, must be scanned for viruses and malware before attaching to any Institutional videoconferencing system.

Event Management System (EMS)

EMS is the Institutional resource reservation management system for scheduling the use of classrooms, conference rooms, telemedicine facilities, videoconferencing services, and certain other resources at TTUHSC. EMS is maintained by a combination of TTUHSC and vendor personnel providing software support, system upkeep, database management, and user training. The TTUHSC I.T. Division is the system owner, administrator, and operational manager; and the CIO is the approving authority for all EMS revisions, upgrades, and configuration changes. The primary point of contact for EMS issues is the I.T. Division Senior Director of Telecommunication Services. See the sections below on Configuration Management and Requests for Change to recommend or request changes of any type to the Event Management System. These may include but are not limited to revisions, upgrades, and changes to features, privileges, and resources. (See also [Security](#) and [Disciplinary Process](#)).

Access to EMS

TTUHSC staff assigned to scheduling duties on behalf of departments and schools use the EMS Client version for creating TechLink resource reservations. The EMS Web Portal is available to individual faculty, staff, and students for requesting the use of TechLink services. Persons needing either type of EMS access should contact the I.T. Division TechLink Network Scheduling Coordinator at (806) 743-7064 for assistance in creating an account.

TechLink Services

Facilities equipped with Institutional videoconferencing systems may be scheduled by customers to provide a range of technology services. Included are distance learning classrooms, videoconference rooms, teaching studios, auditoriums, telemedicine consultation facilities, production studios, satellite earth station facilities, and the I.T. audio bridge. The following TechLink services are provided by the I.T. Division:

- **TechLink Broadcast** (videoconference involving at least two separate endpoints).
- **TechLink Non-broadcast** (use of a room and its videoconferencing system without connecting to another location, i.e., local use).
- **Content Capture and Storage** (recording of TechLink sessions for future access by the customer).
- **Audio Conference** (telephone conference using the I.T. audio bridge).
- **Satellite uplink / downlink services** (broadcast or reception of content via satellite).

TechLink User Assistance

The I.T. Division recommends that customers participate in an appropriate orientation or training program before attempting to use any Institutional videoconferencing system. Available training is listed below, and is intended to enhance the customer's overall TechLink experience.

- **Event Management System user training** – available from the I.T. Division Telecommunication Services Department in Lubbock at (806) 743-7064.
- **TechLink Classroom and Multi-media Teaching Podium user training** – available at all TTUHSC campuses. May be scheduled through the I.T. Division's Education Services Department in Lubbock at (806) 743-1500. (NOTE: Initial user orientation is available from the applicable regional campus TechLink staff for customers who have not yet attended the formal offered by the I.T. Division)
- **Telemedicine Systems user training** – available from the F. Marie Hall Institute for Community and Rural Health in Lubbock at (806) 743-1338.

Configuration Management

Institutional videoconferencing systems are equipped with a standard set of multi-media features available at all TTUHSC campus locations. This ensures equal access to educational, business, medical, and other services by providing consistent functionality and performance from campus to campus. Added benefits include simplified technical support; and lower maintenance and operational costs. The CIO or designee is the approving authority for all configuration changes, and with the exceptions below, users are not permitted to change the standard configuration or functionality by adding, removing, altering or reconfiguring hardware or software. Requests to change an Institutional videoconferencing system, facility, or feature, may be submitted to the

Office of the CIO or the Senior Director of Telecommunication Services (See Requests for Change below). The installation of unapproved hardware or software on Institutional videoconferencing systems, or the intentional alteration, misconfiguration, or removal of all or any part of these systems is a violation of policy (See also [Disciplinary Process](#)).

Exceptions

The following actions by users in the course of their events are not considered unauthorized configuration changes:

- Feature selection and other adjustments regarding user-accessible equipment in the TechLink Multi-media Teaching Podiums. (The I.T. Division encourages users to coordinate these changes in advance with the TechLink Control Center to avoid the potential disruption of network events).
- The loading of content CDs, DVDs, and user files on PCs in the TechLink Multi-media Teaching Podiums. (All user files should be removed at the end of each class or other videoconferencing session).
- The temporary connection of departmental or user-owned laptop PCs and thumb drives to the TechLink Multi-media Teaching Podiums. (The I.T. Division encourages users to include this requirement in their scheduling requests; and to make their laptops available to the I.T. video staff for functional checks in advance of scheduled events. This is to ensure compatibility and proper operation with the teaching podium system due to the wide range of devices available to users).

NOTE: Only designated I.T. Division staff may load application programs on teaching podium PCs, following an operational and security review in which no issues are identified that may interfere with system functionality, privacy, or network security.

NOTE: Departmental and personal media storage devices such as PCs, laptop PCs, thumb drives, CDs, and DVDs, must be scanned for viruses and malware before attaching to any Institutional videoconferencing system.

Requests for Change

Faculty, staff, or students desiring to alter the configuration, features, or functionality of an Institutional videoconferencing system or facility, may submit a written change request to the Senior Director of Telecommunication Services, Information Technology Division, MS 7755 for evaluation. Requests should include the following minimum information:

- Requestor's name.
- Requestor's school or department.
- Requestor's telephone number and e-mail address.

- Description of the proposed change.
- Reason for the proposed change.
- The affected facility and system (such as Odessa RAHC, Room 1C-12, teaching podium).

Following an evaluation of the proposed change, the I.T. Division will respond to the requestor, and if the change is approved, work with the requestor on an implementation plan.

(NOTE: Anyone needing assistance to prepare a change request may contact the Senior Director of Telecommunication Services at (806) 743-1500.

Procurement Review

Videoconferencing equipment, services, and software intended for connection to the TTUHSC network, shall be reviewed and approved by the CIO or designee prior to purchase. (See also [I.T. Procurement Review](#) and the section above on Connectivity.)

Scheduling Priorities for TechLink Facilities and Services

Consistently heavy demand for videoconferencing services at TTUHSC requires the use of these resources to be managed on a scheduled basis according to the priorities and procedures below. This ensures that events receive preferential consideration according to Institutional priorities when conflicting resource reservations occur.

Distance Learning Classrooms:

- Priority 1 - TechLink Broadcast (videoconference) with other endpoints for academic courses of TTUHSC.
- Priority 2 - TechLink Non-broadcast (local use of distance learning classrooms and their installed videoconferencing systems) for academic courses of TTUHSC.
- Priority 3 – TechLink Broadcast for all Institutional events other than academic courses.
- Priority 4 – TechLink Non-broadcast use of distance learning classrooms and their installed videoconferencing systems for any Institutional event.

General Purpose Videoconference Rooms:

- Priority 1 – TechLink Broadcast for any Institutional event.
- Priority 2 – TechLink Non-broadcast use of videoconference rooms and their installed videoconferencing systems for any Institutional event.

Videoconference Rooms Assigned to Administrators, Deans, Departments, and Schools:

- Priority 1 - Internal use by the administrator, dean, department, or school with administrative control of the conference room for any Institutional event.
- Priority 2 – TechLink Broadcast or Non-broadcast use by any TTUHSC student, faculty, or staff for any Institutional event, when approved by the responsible administrator, department head, or dean.

Telemedicine Consultation Facilities:

- Priority 1 – TechLink Broadcast for scheduled or emergency telemedicine consultations.
- Priority 2 – TechLink Broadcast or Non-broadcast use by telemedicine staff for telemedicine education, training, or demonstration purposes.
- Priority 3 – TechLink Broadcast or Non-broadcast use by any TTUHSC faculty, staff, or student for any Institutional event.

Teaching Studios and Auditoriums equipped with videoconferencing systems:

- Same priorities as for Distance Learning Classrooms

NOTE: In the event of an emergency telemedicine consultation when no other telemedicine facilities are available, resources previously scheduled for other broadcast or non-broadcast purposes may be reassigned to accommodate the emergency situation. Time permitting, every effort will be made to inform the organizer of the affected event(s), but such notification cannot be assured.

Scheduling Procedures for TechLink Facilities and Services

Requests to schedule (reserve) TechLink Broadcast and Non-broadcast video services are submitted through the Event Management System. Reservation requests may be submitted on behalf of customers by designated scheduling staff; or directly by the requestor. Designated scheduling staff include the I.T. Division TechLink Network Scheduling Coordinator, regional campus schedulers, and those assigned to scheduling duties within the Classroom Support Department. Persons in these categories should use the EMS Client version; and the EMS Web Portal is available for individual faculty, staff, and students to request TechLink services.

At the Lubbock campus: contact the Classroom Support Department at (806) 743-2288 for assistance, or submit a scheduling request directly through the EMS Web Portal. The Classroom Support Department will forward requests involving TechLink services to the I.T. Division TechLink Scheduling Coordinator for confirmation. Further assistance may be obtained by contacting the I.T. Division TechLink Scheduling Coordinator (806) 743-7064.

At the regional campuses: contact your school or department's administrative offices for the name and telephone number of your regional campus scheduler. This person will forward requests involving TechLink services to the I.T. Division TechLink Scheduling Coordinator for

confirmations. Further assistance may be obtained by contacting the I.T. Division TechLink Scheduling Coordinator (806) 743-7064.

At all campuses, contact the F. Marie Hall Institute for Rural and Community Health in Lubbock at (806) 743-4440, to schedule the use of telemedicine facilities.

At the Lubbock campus, contact the I.T. Division TechLink Scheduling Coordinator (806) 743-7064 to schedule use of the I.T. audio bridge and satellite uplink / downlink services.

Information Required to Schedule TechLink Facilities and Services

When reserving the use of TechLink facilities or services, customers should provide the following minimum essential information to support their requests:

- Event date.
- Event beginning and ending times.
- Requestor information (i.e., the name and telephone number of the person who is scheduling the TechLink services).
- Presenter name and telephone number.
- A list of all campuses and/or other locations to be included in the event (NOTE: for locations outside of the TTUHSC campus system, provide a contact name and telephone number for technical coordination).
- The originating site (location of instructor or presenter) if the event is a TechLinked class.
- A list of special technical needs the Presenter will have including:
 - o Pre-event training in the use of the teaching podium or videoconference room system.
 - o Use of personal laptop (state whether MAC or PC).
 - o Use of CD, DVD, thumb drive, or other device.
 - o Use of the Internet.
 - o Webinar services.
 - o Content capture (recording) services.
 - o Other as may be applicable.

NOTE: for recurring events, provide a listing of all event dates, beginning and ending times, and locations involved, for each event date.

Additional Information Regarding the Scheduling of TechLink Facilities and Services

- Short-notice requirements – to schedule TechLink services Monday-Friday, 8:00am to 5:00pm with less than 2 hours advance notice, customers have the option of using EMS or contacting the I.T. Division TechLink Scheduling Coordinator directly for support. Customers with greater than 2 hours advance notice of their events are asked to use EMS as described above in the section on Scheduling Procedures for TechLink Facilities and Services.
- Telemedicine emergencies – to schedule TechLink emergency telemedicine support Monday-Friday, 8:00am to 5:00pm, contact the TechLink Video Network Control Center directly at 743-7053; 7054; 7060; or 7061.
- Telemedicine emergencies – to schedule TechLink emergency telemedicine support after hours and weekends, contact the On-call technician at 743-7053.
- TechLink connections to locations outside the TTUHSC network, require 2-3 work days advance notice due to the need for equipment compatibility testing.
- After-hours events – a minimum of 14 days advance notice is required to schedule a TechLink event that will be held outside of normal business hours (Does not apply to telemedicine emergencies.)
- Weekend events – a minimum of one month advance notice is required to schedule a TechLink event that will be held on a Saturday and/or Sunday. (Does not apply to telemedicine emergencies.)
- Institutional holidays – TechLink services are not available on official Institutional holidays except for telemedicine emergency support.

Changes to Scheduled Events

The I.T. Division manages the support of TechLink Broadcast and Non-broadcast services through the use of an event schedule which ensures that distance learning classrooms and other video facilities and services are ready for use when needed. Effective customer support can be assured only if the TechLink Event Schedule includes accurate information from users concerning their scheduled TechLink events. This requires that users communicate any changes to their “Confirmed TechLink” events as soon as they become known. Accordingly, changes affecting confirmed TechLink Broadcast and Non-broadcast events should be reported to the Classroom Support Department in Lubbock at (806) 743-2288; or to the appropriate regional campus scheduling staff. Classroom Support and regional scheduling staff should use the “Reminder” feature of EMS to notify the I.T. Division TechLink Scheduling Coordinator of any changes to Confirmed TechLink events received by their department. Only the designated I.T.

scheduling staff is permitted to implement changes to scheduled TechLink events. Examples of reportable changes are listed below.

- Event cancellation.
- Addition or deletion of participating endpoints.
- Change in beginning or ending time of an event.
- Change in event date.
- Change in event duration.
- Change in the origination site of TechLink broadcast events.
- Change in expected group size.

Fee for Service

The use of certain TechLink and other I.T. Division audio-visual facilities and services may result in service charges to the customer. Examples of facilities and services for which these charges may be assessed, include:

- Technical support of after hours and weekend TechLink Broadcast and Non-broadcast events.
- Satellite uplinks and downlinks.
- I.T. production studio services.
- Videoconferencing project support such as consulting, design, procurement, installation, project management, and associated services.
- Operational support of customer owned equipment including onsite maintenance, network technical services, and associated support.

Technical Difficulties

Customers needing technical assistance with an Institutional videoconferencing system during a TechLink Broadcast or Non-broadcast event may contact the local or central TechLink Video Network Control Center by telephone (or directly via the room microphone if the audio link is functioning). Depending upon their location, customers should use one of the following numbers to reach a TechLink Video Network Control Center if calling by telephone:

Lubbock (Central Control): (806) 743-7053; 7054; 7060; or 7061

Abilene: (325) 676-3899 (O); (325) 829-7940 (C)

Amarillo: (806) 356-4629; 806-356-4048

Dallas (VA Campus) (214) 372-2817 (O); (817) 808-5634 (C)

Dallas (Forest Park): (214) 351-2224 (O); (214) 500-6373 (C)

El Paso: (915) 545-6407

Midland: (432) 620-8057

Odessa: (432) 335-5197

All other locations: Use the Lubbock contact numbers

Videoconferencing Systems Security

Institutional videoconferencing equipment, software, systems, and services are subject to the same security rules and policies that govern other electronic communications at TTUHSC. As a further precaution, departmental and personal media storage devices such as PCs, laptop PCs, thumb drives, CDs, and DVDs, must be scanned for viruses and malware before attaching to any Institutional videoconferencing system. (See also Security and Disciplinary Process).

Audits of Videoconferencing Equipment, Systems, and Software

(See also [Security](#)).

3. INSTITUTIONAL COMPUTER NAMING CONVENTION STANDARDS

Computer Naming Convention

To facilitate the easy identification of computers on the network, all TTUHSC computers will be named using the following convention:

- 3-letter city code (e.g., AMA, ELP, LUB, ODE)
- Department code (e.g., IT, SOM, PED)
- 6-digit Tech Inventory number (five digit tag numbers will be preceded by a zero) preceded by the letter “T” (The “T” signifies that the number is a Texas Tech Inventory ID)
- If a Tech Inventory Number is not available, use the manufacturer’s serial number without the letter “T”.
- If the manufacturer’s serial number is longer than 7 digits, use the last 7 digits of the serial number.

For example, a computer in the Lubbock I.T. Division with an inventory tag number of 7893 would be named LUBIT-T078943.

4. HARDWARE AND SOFTWARE STANDARDS

The overall reliability of the HSC Network is the responsibility of TTUHSC Information Technology Division. However, every school, department, and user is responsible for meeting standards that will help ensure this reliability.

Non-standard hardware configurations and software packages normally require additional resources and expertise. Work orders submitted on standardized hardware and software will receive priority service over non-standard hardware and software due to the additional specialization and time required.

For the current configuration recommendation for desktops and laptops, see the I.T. Solution Center's Computer Configurations page here: <http://itsolutions.ttuhs.edu/configurations.aspx>

Supported Software Packages:

[PC Software](#)

[Macintosh Software](#)

To ensure comprehensive dissemination of information, all browser home pages shall be set to the TTUHSC Announcements Page - <http://announce.ttuhs.edu/>.

Even if a machine meets the above requirements, Information Technology reserves the right to remove any equipment attached to the network that may be causing problems. For more detailed hardware and software guidelines, go to the [Information Technology Supported Hardware and Software page](#) or contact the [I.T. Department](#) at your respective campuses.

5. TECHNOLOGY REPLACEMENT SCHEDULE

Technology use at TTUHSC has increased greatly over the years. What was once considered large one-time capital acquisitions where agencies expected to see value from these I.T. purchases over a long period of time is now a recurring operational expense that must be incorporated into the annual Institutional budget.

A PC life cycle illustrates the useful life of a computer from its initial acquisition to its ultimate disposition and should be based on end-user needs, technology changes, as well as the cost to support technology. In an effort to address these issues, the State of Texas has identified what a reasonable PC life cycle should be for state agencies and institutions of higher education.

Based on the Department of Information Resources (DIR) guidelines, the recommended Institutional technology replacement/refresh cycle is set at 4 to 5 years for desktop computers and 2 to 3 years for laptops. This guideline is the recommended standard for all TTUHSC facilities. Functional needs and/or resource availability can result in a shorter or longer replacement cycle at the operational level. However, regardless of the length of the cycle, departments should avoid fragmenting their users' base between different operating systems and application versions.

The effective life cycle for data center servers and storage area network equipment is 5 years.

The effective life cycle of videoconferencing equipment and systems is somewhat different than for PCs and application software. Earlier models continue to have operational value for longer periods than PCs and software because audio and video communication standards are well established and major change occurs less frequently. For these reasons, videoconferencing hardware and software installed in multi-media teaching podiums and similar devices maintained and operated by the TTUHSC Information Technology Division will be replaced when one or more of the following conditions exist:

- Required to meet approved user requests for new or enhanced functionality
- Required due to limited functionality (does not provide the range of features or functions generally accepted to be the standard at the time of replacement)
- Required due to obsolescence (unable to meet approved new or stricter performance standards for audio and video signal quality)
- No longer logistically supportable

The exception is that PCs and application software installed in multi-media teaching podiums will be replaced according to the technology replacement schedule and policy outlined above for those items.

6. I.T. PROCUREMENT REVIEW

With the increased deployment of I.T. resources at TTUHSC, the Institution must strategically review procurements to ensure they are consistent with the Institutional direction to achieve an integrated environment. This policy's intent is to provide guidelines for I.T. procurements and to establish an I.T. procurement procedure that allows the individual departments and schools flexibility in making their technology purchases. Refer to [TAC 216](#) and [HSC O.P. 56.03, Project Management](#), for additional information about I.T. resources and procurement review.

General Principles

The CIO is the delegated authority for establishing I.T. purchasing procedures that comply with the Institutional purchasing requirements and meet the needs of the Institution.

Prior to making I.T. purchases, schools and departments must ensure:

- I.T. products are supported by the Information Technology Division. Specific hardware and software are recommended based on the ability to provide support for them. For a list of supported products, refer to the [Hardware and Software Standards](#) or visit the [Information Technology Supported Hardware and Software page](#).
- I.T. products will not adversely affect the integrity and/or security of the TTUHSC network. (Certain network-related purchases must be pre-approved by the TTUHSC Information Security Officer. Refer to the [Procurement Procedure Section](#).)

In order to standardize the hardware configuration and software packages used in this Institution, schools and departments are strongly encouraged to review the following I.T. recommendations before making any purchases:

- [Hardware Configuration](#)
- [Software Packages](#)

Procurement Procedure

The technology needs of the various schools and departments within TTUHSC are admittedly diverse. While units of the Institution have the flexibility to address their departmental I.T. needs, this policy requires strict adherence to the I.T. procurement guidelines contained herein.

First and foremost, TTUHSC Department of Purchasing rules and regulations govern all Institutional purchases, regardless of the nature of the purchase or the items purchased. Detailed purchasing guidelines can be found in the Department of Purchasing's online [Procurement Manual](#).

In order to ensure the consistency and efficiency of the TTUHSC I.T. environment:

- The CIO or their designee must approve all I.T. purchases in the area of hardware, software, and I.T.-related contracts amounting to \$25,000 or greater.
- Any I.T. purchases that, when utilized, could affect the normal operation and functionality of the I.T. environment must also be approved by the CIO, regardless of the cost. (Network devices such as routers, hubs, and firewalls could affect the security and integrity of the TTUHSC network infrastructure. For example, an unapproved router could cause IP address conflicts when installed on the network, a remote desktop program could inadvertently advertise the availability of an open port on the network, and a non-standard firewall could prevent access to the network even to legitimate users, and unapproved videoconferencing equipment or systems could create compatibility issues that could adversely affect the quality of distance learning and similar videoconferencing sessions on the TTUHSC network.)

Additionally, the TTUHSC Managing Director of Network, Security, and Systems must approve certain network-related hardware and/or software purchases beforehand. These include, but are not limited to:

- Firewalls
- Network IDS
- Host-based IDS
- Virus protection
- Vulnerability assessment
- Servers
- Video bridges
- Video codecs
- Video content capture and streaming devices

For detailed guidelines, refer to the [Security Policy](#).

Procurements that require prior approval must be submitted to the CIO and/or the Information Security Officer prior to submitting the procurement documents to Purchasing or obligating the Institution.

7. INTELLECTUAL PROPERTY RIGHTS

All products created on Institutional property belong to the Institution. These products shall be considered "intellectual property" as defined by and managed according to [Board of Regents Rules and Regulations, Chapter 10 - Intellectual Property Rights](#).

8. COPYRIGHT

Unauthorized duplication of copyrighted information and software packages is a direct infringement of the Federal copyright law. (For further information, please refer to the links provided under the [Federal Statutes](#) sections of this site.)

It is illegal to make, use, or pass along unauthorized copies of software, graphics, music, videotaped material, or any other creative art or intellectual property for multimedia projects or any other use.

For information on privacy relating to educational records and their disclosure (including directory information), see the [Family Educational and Privacy Rights Act](#) (also known as the Buckley Amendment) under the [Federal Statutes section](#) of this site.

Computer Software

Copying, adapting, and/or electronically transmitting computer software is strictly forbidden except:

1. Where a new copy or adaptation is created as an essential step in the utilization of the computer program in conjunction with a new machine and that it is used in no other manner.
2. Where a new copy and adaptation is for archival purposes only and that all archival copies are destroyed in the event that continued possession of the computer program should cease to be rightful.
3. Where appropriate, written consent (from the holder of such copyright) is obtained.
4. Where the software is in the public domain, and appropriate documentation can be supplied.

As with CD's and DVD's, computer programs may not be rented, leased, or loaned for direct or indirect commercial advantage.

Lawful transfer of possession of a legally licensed computer program may be exempt, provided there are no existing copies left on the original machine.

TTUHSC prohibits the unauthorized copying or electronic transmission of computer software, computer data, software manuals, videotaped materials, and other multimedia items unless appropriate written consent is obtained from the vendor and/or copyright holder.

8.1. COPYRIGHT AND COMPUTER SOFTWARE

Copying, adapting, and/or electronically transmitting computer software is strictly forbidden except:

1. Where a new copy or adaptation is created as an essential step in the utilization of the computer program in conjunction with a machine and that it is used in no other manner.
2. Where a new copy and adaptation is for archival purposes only and that all archival copies are destroyed in the event that continued possession of the computer program should cease to be rightful.
3. Where appropriate, written consent (from the holder of such copyright) is obtained.
4. Where the software is in the public domain, and appropriate documentation can be supplied.

As with CD's and DVD's, computer programs may not be rented, leased, or loaned for direct or indirect commercial advantage.

Lawful transfer of possession of a legally licensed computer program may be exempt, provided there are no existing copies left on the original machine.

8.2. INFRINGEMENT OF COPYRIGHTS ON COMPUTING SOFTWARE

TTUHSC prohibits the unauthorized copying or electronic transmission of computer software, computer data, software manuals, videotaped materials, and other multimedia items unless appropriate written consent is obtained from the vendor and/or copyright holder.

9. WEB STANDARDS

With the proliferation of Internet use and given the importance of the Internet as a communications forum, it is increasingly important to establish guidelines that protect the Institution from liability while extending the Institution's visual identity to include online publishing. All web and application development must comply with the security guidelines and coding practices set forth in Policies [1.4.20](#), [9.3](#), [9.4](#), and [9.5](#).

9.1. STUDENT WEB PUBLISHING STANDARDS

TTUHSC recognizes the value of publishing on the Internet and supports students in creating personal or curricular web sites and/or web pages. Free personal student accounts are available through the I.T. Division and are allocated 40MB of server space per account. Students needing help setting up their web site and/or web page can contact the TTUHSC Information Services in Lubbock at (806) 743-1500 for assistance. For more information and/or instructions on obtaining student web space, go to the [Student Web Server page](#).

While student web sites and/or web pages are considered “unofficial,” the quality of the information published will still affect the reputation and image of TTUHSC. To prevent any negative impact to the Institution, the following web publishing standards have been established for student web sites and/or web pages:

1. All student web sites and/or web pages must comply with the TTUHSC [Acceptable Use Policy](#).
2. TTUHSC will maintain and support the central web environment. Students are responsible for editing, uploading, debugging, and maintaining the content of their own sites and/or page.
3. Texas Tech logotypes and any other official logos may only be used in web documents by schools, departments, and administrative areas. Unofficial web sites and/or web pages are not allowed to display any official logotypes.
4. All web publishers/authors must abide by the copyright laws, regardless of whether the site/page is an official or unofficial one. Refer to the [Web Use and Copyright Section](#) for more detailed guidelines.
5. Student web sites and/or web pages are considered “unofficial” and must be identified as such with [disclaimer notices](#). All unofficial web sites and/or web pages must prominently display the [Notice of Disclaimer for Unofficial Web Sites/Pages](#).
6. To avoid unnecessary scrolling, all web sites and/or web pages should be sized no larger than 1024 x 768 pixels. The best practice is to design the page no larger than 900 pixels wide.
7. Graphics should be in the GIF, JPEG/JPG, or PNG format with a maximum resolution of 72 dpi/ppi. Higher resolution graphics will make the site/page unnecessarily slow to load. If the graphic needs to be resized or resampled, a graphic program should be used rather than manipulating it through the HTML graphics size elements to ensure that the graphic will remain clear, crisp, and fast to download. For the best quality, it is recommended using the original graphic to modify then re-export as a GIF or JPG as necessary.
8. Include Alt Tag descriptions when using graphics to ensure persons unable to view the graphic or persons using a text browser will be able to understand and navigate the site and/or page.
9. All student web sites and/or web pages should include a footer section that provides:
 - A link to the TTUHSC home page
 - The site/page owner’s name and email address
 - Notice of Disclaimer For Unofficial Pages

These necessary footer codes may be found on the [Student Web Server page](#).

10. Personal sites and/or pages will be removed 6 months after a student’s last semester at TTUHSC, unless special arrangements are made between the student and Information Services.

For questions or comments regarding these requirements, contact it.webmaster@ttuhsc.edu.

Below is a list of recommended design and procedural standards for student web sites and/or web pages:

1. Before making any document public, spell check, and proof read first.
2. Update contents regularly and check all links to ensure they are in working order.
3. Avoid using large graphics. It will make the page load time unnecessarily long. Consider, instead, using a thumbnail where appropriate. If linking to large files or graphics, add a warning statement to prepare the user for the extended load time.
4. Use a template or style sheet to ensure visual consistency across the web site and/or web page.
5. Provide a link to the parent page on all supporting pages.
6. Avoid browser-specific elements.

All web accounts will be subject to monitoring and audits by the I.T. Division for compliance with the policies contained herein. TTUHSC reserves the right to remove any web site and/or web page found to be in violation of TTUHSC, Federal, State, and/or local rules, policies, or procedures. A removal notification will be sent out to the registered web publisher 30 days before the site and/or page is removed and a second notice will follow 10 days prior to the removal date. However, a site and/or page may be removed immediately with the approval of the CIO.

9.2. TTUHSC WEB PUBLISHING STANDARDS

Web content should be in the best interest of TTUHSC and not conflict with the [mission](#) of the Institution. TTUHSC encourages its schools, departments, and administrative areas to utilize web publishing whenever possible to accomplish their goals and support the mission of the Institution.

The quality of the information published on the web directly affects the reputation and image of TTUHSC. In order to prevent any negative impact to the Institutional reputation and image, the following Institutional web publishing standards should be observed:

- The department head or their designee within the school, department, or administrative area must approve all official web publications prior to publication.
- The content and links of all web sites and/or web pages are the responsibility of the web author and their respective departments and/or organizations and should be reviewed/updated on a recurring basis according to the guidelines set forth by the Web Strategy Council to ensure their accuracy.

Sites and/or pages that are not regularly maintained or whose content is deemed outdated by the Associate VP of Information Services may be subject to removal. A removal notification will be sent out to the registered web publisher 30 days before the site and/or page is removed and a second notice will follow 10 days prior to the removal date. However, a site and/or page may be removed immediately with the approval of the CIO.

- Texas Tech logos are legally protected trademarks and unauthorized use of these trademarks is prohibited. The use of Texas Tech logotypes must remain consistent to

provide a strong Institutional identity across the Internet. All TTUHSC Official Seals and Logos for the website and web pages are implemented in the templates and layouts of the Content Management System. In cases where the Content Management System is not used, other software may be used to manage templates. Altering the logos and lock-ups are prohibited. For print and other uses, the logos and lock-ups must be obtained from the Official Identities area of the [Visual Identity Guideline web site](#) for print and other uses.

- Web publishers/authors must take into account and abide by the appropriate copyright laws. Refer to the [Web Use And Copyright Section](#) for more detailed guidelines.
- Official web sites and/or web pages should not contain links to sites and/or pages devoted to individual hobbies or interests.
- TTUHSC encourages students and student organizations to publish web sites and/or web pages. These web sites and/or web pages are considered unofficial and must be identified as such by displaying the [Notice of Disclaimer for Unofficial Web Sites/Pages](#) in the footer section on the site/page.

All TTUHSC web sites and/or web pages must comply with [Texas Administrative Code 206](#) - State Web Sites for accessibility, usability, privacy, security, etc. See the following for more information:

- [State of Texas Web Publishing Standards](#)
- [Texas Administrative Code 206-State Web Sites](#)
- [W3C's Web Accessibility Initiative](#)
- [W3C Web Content Accessibility Guidelines 2.0 Quick Reference](#)
- [DIR's Statewide Electronic and Information Resources \(EIR\) Accessibility](#)
- [DIR's SRRPUB11 State Web Site Guidelines](#)

The following elements are required for all Texas Tech University Health Sciences Center web sites and/or web pages:

- Official sites and/or pages must include an identifier that associates it with TTUHSC which includes the TTUHSC logo, title text that identifies the site and/or page. Refer to the [Web Site Visual Elements Standards](#) for more information.
- Unofficial web sites and/or web pages, such as student organization or student personal sites and/or pages must be identified as "unofficial" and must display the [Notice of Disclaimer for Unofficial Web Sites/Pages](#).
- Web sites and/or web pages must identify a contact person who is responsible for the content of the material. That person's name, e-mail address and school, department, or administrative area should be included at the bottom of the web site and/or web page.
- Official web sites and/or web pages must display the [Notice of Disclaimer of Liability for Official Web Sites/Pages](#) and comply with the requirement listed in the [Web Site Visual Elements Standards](#).
- For additional requirements, see [Section 9.8 for the State of Texas Web Publishing Standards](#).

All TTUHSC web sites and/or web pages are expected to adhere to the highest level of quality and abide by these web publishing guidelines.

1. TTUHSC web sites are expected to follow the zone layout guidelines presented in [Policy 9.4](#) and comply with the color and typography standards for web sites that are outlined in the [Visual Identity Guidelines](#). For the text on the web sites, the font should be Arial. The Visual Identity Guidelines are implemented in the templates and layouts of the Luminis Content Management System. To establish a web site outside of these guidelines, a request should be submitted to the Associate Vice President for Information Services and the Director of Communications and Marketing so that it can be presented to the President for review and approval.
2. **TTUHSC web sites and web pages should be designed to fit a 1024 x 768-screen resolution.** In order to comfortably fit this size screen with no side scrolling, it is recommended that the layout should fit within the width of 900 pixels.
3. **All graphics that are used on the web sites and/or web pages must be formatted as follows:**
 - a. Graphics Interface Format (GIF), PNG, or Joint Photographic Experts Group (JPEG/JPG) file formats only. (GIF is a graphic file format that uses indexed color graphics and supports up to 256 colors with lossless compression. It is best used for flat images. JPEG/JPG is a graphics file format typically used to display photo-realistic pictures that contain thousands or millions of colors. Portable Network Graphics (PNG) is a bitmapped image format and video codec that employs lossless data compression and supports palette-based images.
 - b. Maximum resolution of 72 dots-per-inch (dpi) or pixels-per-inch (ppi) for each graphic. (DPI and PPI is a measure of sharpness or density of illuminated points on a display screen.) Higher resolution graphics will make the download time unnecessarily long. Alternatively, a thumbnail may be used as a link to a separate higher resolution image.
 - c. All TTUHSC Official Seals and Logos for the website and web pages are implemented in the templates and layouts of the Content Management System. In cases where the Content Management System is not used, other software may be used to manage templates. Altering the logos and lock-ups are prohibited. For print and other users, the logos and lock-ups must be obtained from the Official Identities area of the [Visual Identity Guidelines](#) web site.
 - d. When sizing graphics, a graphic program should be used to resize and resample the graphic file, rather than using the HTML graphic size elements for this purpose. This will ensure that the graphic will be clear, crisp, and does not take an inordinate amount of time to download. For the best quality, it is recommended using the original graphic to modify then re-export as a GIF or JPG as necessary.
4. Publishing Documents on State Web Site Standards. Documents shall be organized so they are readable without requiring an associated style sheet. The Adobe Acrobat family of products has built upon the accessibility features first introduced with version 5.0. These improvements address both the needs of individuals with a variety of disabilities and providers with an interest

in creating accessible documents. For an overview of accessibility features in the Adobe Acrobat family of products, visit <http://www.adobe.com/accessibility/products/acrobat>.

9.4. CHANGE MANAGEMENT PROCEDURES FOR OFFICIAL TTUHSC WEB PAGES/SITES

Templates have been used to manage and maintain the web site layout and navigation. Within a web page, a specific command can be used that will insert the contents of another file (the include file) into that web page. This is especially useful when template components, such as headers, footers, and navigational elements, are the same on a number of pages throughout a Web site. Using include files allows a programmer to only modify the include file to change a template element, instead of updating every individual Web page. Include files have been used primarily to maintain consistent navigation.

The web design attempts to maintain a consistent navigation. To this end, much of the navigation has been integrated on related pages. Navigational integration exists in situations where a navigational set is deemed important enough to be repeated from page to page. An example of this is the integration of HSC resources and other global navigation into every page. At the department level, integrated navigation exists for that department only. In order to manage and maintain the integrated navigation, include files have been utilized.

Within the templates, areas have been designated as “not editable” and “editable”. “Editable” areas are controlled by the appropriate content managers unless it is noted differently in this procedure. “Not editable” areas and include files that are used for integrated global navigation are controlled primarily by the Web Strategy Council and their appointed work groups unless it is noted differently in this procedure.

Development and Oversight

An integrated information environment that enhances education, research and patient care at TTUHSC requires resources dedicated to the development, implementation, and support of TTUHSC’s Web Presence. The development and oversight of TTUHSC’s Web Presence including the web sites, the portal, and content management will be under the leadership of the Web Strategy Council. One member will be appointed to the Web Strategy Council by the:

- President,
- Executive Vice President for Finance and Administration,
- Executive Vice President for Research,
- Senior Vice President for Academic Affairs,
- Vice President for Information Technology and CIO,
- Vice President for F. Marie Hall Institute for Rural and Community Health,
- Dean of the School of Allied Health Sciences,
- Dean of the TTUHSC School of Medicine,
- Dean of the Foster School of Medicine,
- Dean of the Anita Thigpen Perry School of Nursing,
- Dean of the School of Pharmacy,
- Dean of the Graduate School of Biomedical Sciences
- Director of Communications and Marketing

- Assistant Vice President for Finance and Administration, Amarillo,
- Assistant Vice President for Finance and Administration, El Paso,
- Assistant Vice President for Finance and Administration, Permian Basin, and
- TTUHSC Student Government Association President.

The CIO or his designee will chair the Web Strategy Council. The Web Strategy Council will meet formally on an annual basis or more frequently at the call of the CIO or his designee. The Council will also meet electronically through the use of SharePoint or other methods to conduct business as needed. The Web Strategy Council will provide the leadership and expertise needed for TTUHSC to develop a coordinated web strategy. Under the direction of the CIO, the Council will serve as the advisory body reporting to the I.T. Board of Directors to:

- Define the goals and objectives for the web site,
- Create web policies and standards,
- Recommend procedures to ensure compliance with web policies and standards,
- Create a strategically integrated web environment for TTUHSC,
- Coordinate web activities throughout TTUHSC,
- Provide seamless access to information and services throughout the web domain,
- Provide direction and governance for the HSC Luminis Web Portal,
 - Recommend new HSC and Texas Tech channels and enhancements to the project prioritization committees
 - Recommend new HSC links
 - Evaluate other institutions' Portals on an ongoing basis for content and usage ideas
 - Review and approve/deny requests for channels and links within the portal made by HSC entities
- Recommend appointments of specific content organization groups when needed,
- Approve Tier 2 and lower template designs,
- Define site development and maintenance responsibilities for TTUHSC web sites through the recommendation of appointments of content contributors and content managers for each department, school and campus,
- Establish design and content lifecycles, and
- Provide an Institutional approach to skills development and the acquisition of software tools.

The current lifecycles as approved by the Web Strategy Council on June 13, 2006 are:

- Design - The current structure and navigation will begin to be reviewed in 2 years.
- Content - All content will be reviewed at least yearly.
- Central Column - The middle content area on the Institutional home page, that includes the "From Here It's Possible," "Prepare for Your Future," and "Make an Impact" areas, will be reviewed every 6 months.

Modifications To "Not Editable" Areas In All Templates

Modifications to the "not editable" areas of the templates are managed by the following process:

- Design is approved by the President's Executive Council (PEC), the Web Strategy Council provides leadership in development and oversight, and Information Services maintains design and layout.
- The design of the web site will be reviewed on a recurring basis as defined by the Web Strategy Council.

Requests for possible modifications to the design or navigation must be submitted to the Web Strategy Council through the Associate Vice President of Information Services. Modification requests will be considered by the Web Strategy Council (WSC) as necessary. The modification requests that were accepted for approval by the WSC are referred to the PEC for final approval. All requests must be approved by the PEC prior to implementation.

Institutional And Campus Home Page Management - "Editable" Areas

The current web design for TTUHSC is based upon the zone layouts described in this section of the I.T. Policies.



Because the Institutional and Campus home pages represent the entire TTUHSC community, quality assurance is necessary to retain the integrity of the Institution’s identity. Therefore, modifications to the “editable” areas on these pages are managed by the following process:

Zone 4 - “Prepare for Your Future” and “Make an Impact” and Zone 5 - News and Announcements and Features Areas

The Office of Communications & Marketing (OCM) at the Institution or the campus manages the information and marketing aspect of these areas. All text, photos, and links must be submitted to OCM for approval prior to posting.

All other zones contain “not editable” areas only:

Zone 1 - Logo

Zone 2 - Search

Zone 3 - Audience Menus and Health Science Center Menus

Zone 6 - Footer

Key Public Entry Point Page Management- “Editable” Areas



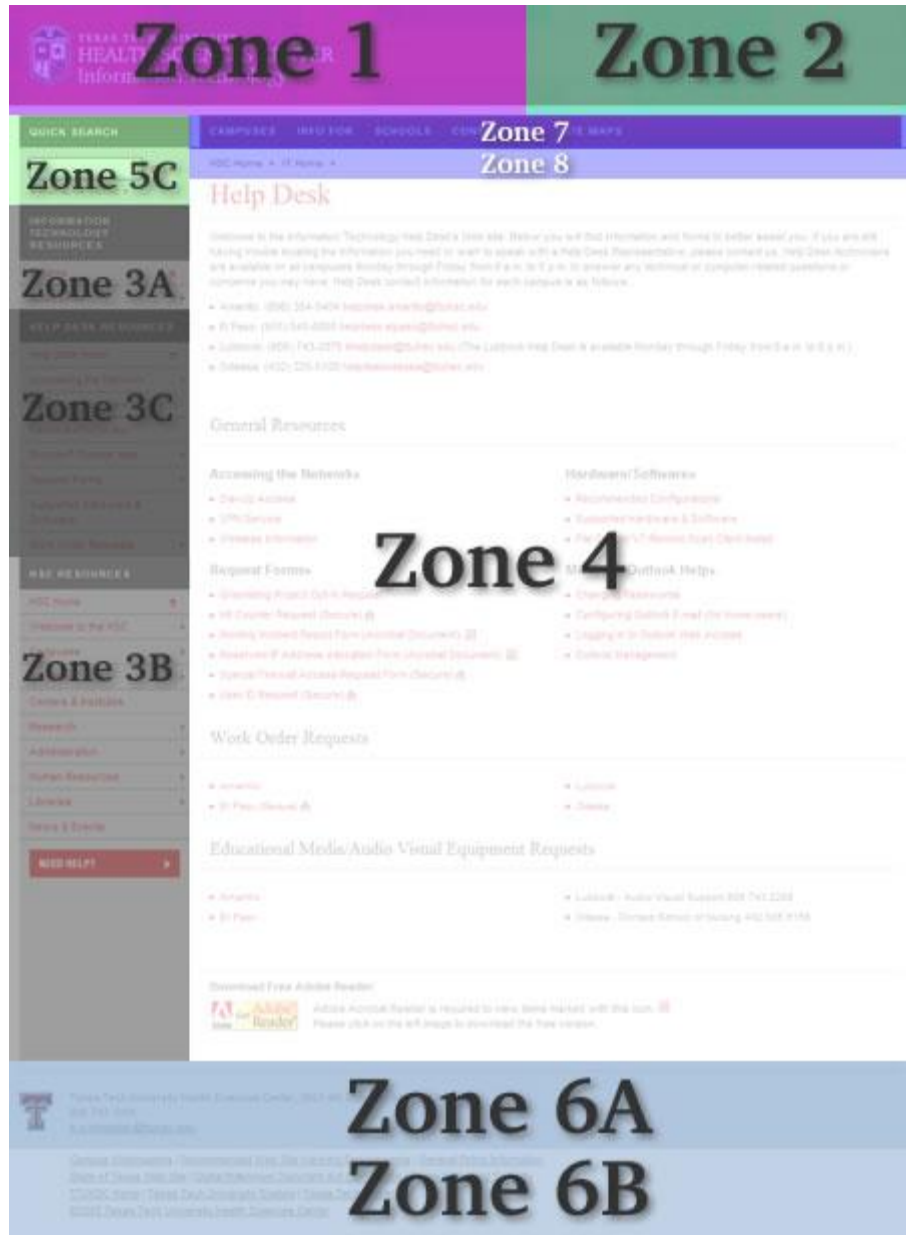
A [key public entry point](#) is defined as a web page that is specifically designed for members of the general public to access official Institution information. TTUHSC has designated the following as key public entry points:

- Audience home pages,
- School home pages, and
- Offices and other administrative areas.

Key public entry points represent high profile areas of the TTUHSC web, thus quality assurance is necessary to retain the integrity of the Institution's identity. At these levels, upper level navigational elements are interconnected. The interlocking nature of this navigation ensures consistent and up-to-date access to high-profile information. Modifications to "editable" areas on key public entry points are managed by the following process:

- **Zone 3A and 5A - Audience/School/Office or Administrative area navigation**
 - Each entity is responsible for modifications to their navigation area.
- **Zone 5B - Audience/School/Office or Administrative area Announcements or news**
 - Each entity is responsible for modifications to their navigation area.
- **Zone 4 - Entry Area**
 - Each entity is responsible for managing the content of this area.
- **All other zones contain "not editable" areas only:**
 - **Zone 1 - Logo**
 - **Zone 2 - Blank**
 - **Zone 3B - Audience Menus and Health Science Center Menus**
 - **Zone 5C - Search**
 - **Zone 6 - Footer**

Sub Page Management - "Editable" Areas



Because the sub pages are connected to their key public entry points, quality assurance is necessary to retain the integrity of the Institution’s identity and navigation. Modifications to the “editable” areas on sub pages are managed by the following process:

- **Zone 3A & 3C - Audience/School/Office or Administrative area navigation**
 - Includes entities such as Administration, Human Resources, Libraries, News & Events, and Research.
 - Each entity is responsible for modifications to their navigation area.
- **Zone 4 –**
 - This zone is reserved for the page content.
 - Content owners are responsible for maintaining the content of each sub page.

- All content must comply with TTUHSC Operating Policies and Procedures and TTUHSC Identity Guidelines.
- **Zone 6A –**
 - This zone includes the contact information specific to that sub page.
 - The contact information portion of this zone is the responsibility of the content owner.
- **Zone 7 –**
 - This zone includes the Institutional global navigation. An entity may append to the end of the Contact Info and Site Maps lists with links to their respective contact information and site map.
- **Zone 8 –**
 - This zone is used for navigational breadcrumbs. HSC Home is built in the template to always appear as the first part of breadcrumb navigation on a sub page.
 - Subsequent links should reflect the hierarchy of preceding pages, but should never contain the link of the page being displayed.
- **All other zones contain “not editable” areas only:**
 - **Zone 1 - Logo**
 - **Zone 2 - Blank**
 - **Zone 3B - Audience Menus and Health Science Center Menus**
 - **Zone 5C - Search**
 - **Zone 6B - Footer**

General Process For Web Content Management

The purpose of web content management is to preserve the integrity of the TTUHSC web site while maintaining accurate and up-to-date subject matter.

Web management is about facilitating and encouraging the use of the web. This means finding a way to enable non-technical staff to publish web-based materials without too much effort, and yet ensuring quality content that will be useful and effective. Web content management addresses the following questions:

- Who has access to publishing on the web and how is access granted and managed?
 - The Deans, Vice Presidents, Chairs, and Department Heads will appoint content managers and identify content contributors for each campus, school, and department. Information Services will maintain a database of all individuals who have been granted access to contribute and manage content on the web. Information Services will also periodically monitor the compliance of the sites on the TTUHSC web to ensure that they are being maintained in a manner that maintains the integrity of the template design. Anyone not maintaining the integrity of the templates or making unauthorized changes to the design may have their access revoked. After the first or second occurrence, a warning will be sent out to the registered individual and retraining will be scheduled if needed. All access will be revoked upon the third occurrence. However, access may be

revoked immediately with the approval of the CIO upon consultation with the appropriate Dean or Vice President.

- What type of materials can be published?
 - Generally, materials such as word docs, pdf's, excel spreadsheets, text and images may be published. However, all content must comply with the standards set forth in this document and with the TTUHSC Operating Policies and Procedures.
- Who is responsible for content and maintenance?
 - Accountability for high quality content on TTUHSC web sites is a shared responsibility. Each academic or administrative unit will be required to develop and maintain high-quality, up-to-date, easily navigated content applicable to the purpose of the web page or site.
 - Designated content managers are responsible for maintaining accurate and up-to-date subject matter for web pages in their area.
 - Information Services will periodically conduct reviews to insure that web content and brand identity is being kept up to date. Content managers may be contacted in instances where it is noted that content has not been reviewed in the past 12 months. Sites and/or pages that are not regularly maintained are subject to removal. A removal notification will be sent out to the registered web publisher 30 days before the site and/or page is removed and a second notice will follow 10 days prior to the removal date. However, a site and/or page may be removed immediately with the approval of the CIO upon consultation with the appropriate Dean or Vice President.
- What tools are used to create and edit web content?
 - Non-technical content managers will use the content management system to create and edit web content.
 - Technical content managers can also use the content management system to create and edit web content. Alternatively, technical users are also allowed to use such tools as Adobe Dreamweaver, Visual Studio.Net, etc. to create and edit web content and/or develop applications.
 - All content managers will also be required to use the HSC Application Publisher for publishing a web application to production servers. For simple applications and web sites not in the content management system, alternative tools are provided for publishing to the test and production servers. Database driven applications or content will utilize Microsoft SQL Server databases. No other database systems (MS Access, mySQL, etc.) will be allowed on the production web environment without prior approval of the Associate Vice President of Information Services.
 - It is recommended that all application developers utilize a source code repository and versioning tool. Information Services utilizes Team Foundation Server for this purpose. Outside departments may utilize TFS by purchasing the applicable license for use with Visual Studio. For TFS licensing information, please contact Information Services.
- Training and technical support required?
 - Before content managers are given access to their site, they must be trained by Information Services on the following:
 - Use of the Content Management System.

- Use of the HSC Application Publisher and the TTUHSC design templates. If other Information Services developed tools are used for publishing, then training will be required.
- Use of the Microsoft SQL Server test and production environments, if used.
- Use of the design CSS and properly applying style classes as defined in the design stylesheets.
- Coding valid XHTML.
- Complying with American Disability Act (ADA) standards.
- Texas Administrative Code (TAC) compliance.
- Information Services does not provide training on third party products such as Adobe Dreamweaver. Users who choose to use these products in lieu of the content management system are responsible for obtaining training and technical support from other sources.
- How do I make changes?
 - Definitions:
 - Test server - this is the server where all modifications are made and tested prior to moving them to the production server. The test server is only accessible from within the TTUHSC network (<http://wip.ttuhs.edu> for the content management system).
 - Production server - this is the live, publicly accessible version of the web site (<http://www.ttuhs.edu>)
 - All changes to web content are to be made and thoroughly tested on the Institutional test server.
 - All content managers must conduct the “Pre-Publishing Checks” listed below prior to publishing any content from test to production.
 - Access to content on the test servers and the ability to publish to the production servers will be controlled through authentication that utilizes eRaider.
- Pre-Publishing Checks
 - Before publishing a content modifier must:
 - Thoroughly review and test all changes using the test servers provided.
 - Verify that all links within the content are valid.
 - Spell check all pages.
 - Complete Security Code Review and Vulnerability testing with designated Information Services Staff.
- Before publication, validate the page using an acceptable tool or method for:
 - Accessibility
 - Valid HTML or XHTML coding
 - Valid CSS
 - Compliance with ADA standards
 - W3C

If unsure, please contact chris.barnard@ttuhsc.edu

Please note that these processes may change periodically as the TTUHSC web services mature and as movement is made toward a content management system.

9.5. INFORMATION SERVICES CODING STANDARDS, SECURITY, AND AUDIT CONTROLS

1. All application development including web applications will have audit capabilities that will allow the construction of a transaction record of activities.

2. All developers will be familiar with and follow the standards and practices outlined in the following Microsoft Developers Network Resources:

- [Building secure ASP.NET Applications: Authentication, Authorization, and Secure Communication](#)
- [Building Secure ASP.NET Applications: Authentication, Authorization, and Secure Communication - Data Access Security](#)
- [Improving Web Application Security: Threats and Countermeasures](#)
- [Patterns and Practices Security Guidance for Applications Index](#)
- [An overview of Security in the .NET Framework](#)
- [Defend your Apps and Critical User Info with Defensive Coding Techniques](#)
- [.NET Security](#)

Note: Although Microsoft has released their new .NET framework and list this content as "retired", the concepts and practices are still applicable.

3. All developers will periodically review the materials at the following sites as part of their training and skills development.

- MSDN Security Site - <http://msdn.microsoft.com/security/>
- TechNet Security Site - <http://www.microsoft.com/technet/security/default.mspix>

4. All developers will periodically participate in Microsoft Security Training Events as part of the on-going training and skills development. Available events can be located at: <http://www.microsoft.com/events/security/default.mspix>.

5. Typical Development Phases and Steps to follow (SDLC):

- Planning
 - Meet with department
 - Gather requirements
- Analysis/Design
 - Content gathering by department
 - Content organization
 - Navigation Organization
 - Application design (User interface, etc.)
 - Database design
- Development/Testing
 - Create content pages
 - Content graphics
 - Navigation implementation
 - Application programming

- Database development
- IS testing
- Department testing
- Edits/modifications
- Re-test
- Implementation
 - IS approval
 - Department approval
 - Other applicable approvals (HIPAA Privacy Officer, Security Officer, etc.)
 - Compliance Review (TAC, accessibility, etc.)
 - Security Code Review
 - Move to production
 - Content pages
 - Graphics
 - Database
 - Database schema
 - Data migration/creation
 - Application pages
 - Implement SSL (if applicable)
 - Implement authentication (if applicable)
 - Post implementation testing/review
 - Post implementation edits/modifications
 - Final testing/review
 - Final IS approval
 - Final department approval
- Support/Maintenance

6. All developers will utilize the following tools:

- Test Environment -
Visual Studio and HSC Application Publisher for web application development/maintenance. It is recommended that all application developers utilize a source code repository and versioning tool. Information Services utilizes Team Foundation Server (TFS) for this purpose. Outside departments may utilize TFS by purchasing the applicable license for use with Visual Studio. For TFS licensing information, please contact Information Services.

For static content, the content management system is typically used. However, there are instances where it is acceptable to develop/maintain static content with other tools such as Dreamweaver.

For simple applications and web sites not in the content management system, alternative tools that were developed by Information Services will be used for publishing to the test and production servers.

- Production Environment -
All developers will publish to the production environment using the HSC Application Publisher.
 - Content Management System -
All content contributors and managers will use this system to develop, maintain, and publish static content to the TTUHSC web sites.
Note: For simple applications and web sites not in the content management system, alternative tools that were developed by Information Services will be used publishing to the test and production servers.

7. Prior to writing any code or purchasing any software/system at TTUHSC, all developers will:

- Document the requirements and functionality of a development project.
- Review the documented requirements and functionality with the individual(s) or department requesting the development project.
- Insure that they have a thorough understanding of the development project requirements and functionality
- Obtain central IS administrative approval to begin the coding process and determine Project Management needs.

8. All developers will thoroughly test all code prior to implementation.

9. All developers will require the requesting individual(s) or department to perform extensive testing of all code prior to implementation.

10. Developed projects or purchased software/systems will not be moved into the production environment until:

- All code has been thoroughly reviewed and tested. This includes conducting compliance and security code reviews.
- Approval has been obtained from the requesting individual(s) or department and a time frame for production implementation has been agreed upon.
- Production implementation procedures and requirements have been outlined. These include, but are not limited to:
 - Changes to IIS
 - Database structure and data migration
 - Access privileges
- Approved by central IS Management and if applicable HIPAA Privacy and Institutional Security Officers.

11. Web publishing from Test to production

- The HSC Application Publisher will be used to publish content from Test to Production for web applications.
- The content management system will be used to publish static content from Test to Production.

- Simple applications and web sites not in the content management system will utilize alternative tools that were developed by Information Services for publishing to the test and production servers.
- Training on the use of these systems will be provided by Information Services.

9.6. E-COMMERCE APPLICATIONS

- An e-Commerce Service request must be submitted for all e-Commerce applications. A request form may be obtained by contacting Information Technology.
- All e-Commerce service requests and applications must be approved by the Associate Vice President for Information Services, Accounting Services, and Institutional Compliance (if applicable).
- All e-Commerce applications must utilize the Texas Tech University System eCommerce framework.
- All TTUHSC web pages that access the Texas Tech University System e-Commerce framework must be hosted in the central Data Center and will undergo periodic PCI compliance scanning.
- The development of all e-Commerce applications will follow the applicable guidelines outlined in Policies [1.4.20](#) and [9.5](#).
- The requesting department may develop the application to the point of integrating it with the e-Commerce framework. However, only Information Technology personnel may perform the work of integrating the application with the Texas Tech University System e-Commerce framework.

9.7. WEB USE AND COPYRIGHT STANDARD

The use of TTUHSC web and computing resources is a privilege granted by TTUHSC and the State of Texas and is intended to further the educational missions of the Institution. Each school, department, administrative area, and user is responsible for using the TTUHSC web and computing resources ethically, courteously, and lawfully in accordance with the [Acceptable Use Policy](#).

This Institution is committed to making the TTUHSC web a premier part of the Internet that upholds the highest ethical standards and abides by Institutional policies and State and Federal statutes regulating the use of the Internet and protecting the copyrights of others. Web authors are responsible for ensuring the information they publish is free from copyright restrictions and complies with the guidelines set forth in this document.

9.8. STATE OF TEXAS WEB PUBLISHING STANDARDS

All official TTUHSC web sites and/or web pages must comply with the [Texas Administrative Code Section 206 - State Web Sites](#).

The composition of the footer on the TTUHSC web site is incorporated into the Content Management System templates. Information Services will maintain the links within the footer.

Information pertaining to [TAC § 206 - State Web Sites](#) and the links that are required for the TTUHSC footer are available on the [TTUHSC TAC Information page](#).

10. DISCIPLINARY PROCESS

Open access to TTUHSC information technology resources is a privilege subject to appropriate use. Observation of a violation of the policies contained herein will be reported to the appropriate departmental administrator and/or to the CIO, Managing Director of Technology Services, AVP of Information Services, and AVP of Human Resources.

The Information Technology Division shall investigate and review all complaints or instances of unacceptable use brought to its attention. Suspected or known misuse of information technology resources may, pending the result of a thorough investigation, result in, but are not limited to, the following disciplinary actions:

1. Temporary/permanent revocation of user privileges.
2. Suspension/dismissal from the Institution (regardless of any employment contract or tenure status).
3. Restitution for damages.
4. Prosecution under all applicable statutes.

Any restrictive and/or disciplinary actions taken by TTUHSC authorities will be in accordance with guidelines and procedures set forth in Institution policies, codes, or laws. See HSC OP's [70.31](#) and [77.05](#) and the [Student Affairs Handbook](#) for more information.

In addition to this policy, all existing Federal, State, and Institution laws, regulations, and policies apply, including not only those laws and regulations that are specific to computers and networks, but also those that apply to personal conduct.

1. **Access Point** is a device that allows computers or workstations to access the wired network by using radio transmissions. An access point contains transmit and receive antennas instead of ports for access by multiple wireless clients. Similar to standard wired "hubs," access points are shared bandwidth devices.
2. **Authentication** is the process of securing the identity of an individual based on a user account name and password. Authentication ensures the individual is who he or she claims to be, but does not address the access rights of the individual.
3. **Authorization** is the process of assigning individuals the permission to read, write, or modify system objects or execute transactions based on their identity.
4. **Broadcast Messages** are messages that are simultaneously sent out to multiple recipients.
5. **Cable (also referred to as cable modem)** is a type of Internet connection provided by the local cable company, used to transfer data at high speeds when compared to a dial-up modem.
6. **Chain Letters** are letters or emails directing the recipient to send out multiple copies so that its circulation increases exponentially.
7. **Computer Incident Response Team (CIRT)** is comprised of personnel responsible for coordinating the response to computer security incidents in the organization. Regular members will include:

- Chief Information Officer or designee
- Associate Vice President, Technology Services
- Computer Security Analysts

Depending on the nature and severity of the incident, the CIO or designee may appoint additional members to the CIRT from one or more of the following areas:

- Other I.T. staff members with expertise in various operating systems and platforms
- Human Resources representative
- Physical Plant representative
- Texas Tech Police
- Media or public relations liaison

8. **Computer Security Analyst (CSA)** is an individual designated by the Information Technology (I.T.) Director at each campus location. The CSA will be appointed for each TTUHSC regional campus and will coordinate virus protection activities at each campus under the direction of the Information Technology Security (ITS) group. The regional CSA will work closely with the Institutional Information Security Officer to implement security procedures, maintain locally administered security products, respond to security incidents, and coordinate the installation of patches on servers and workstations to correct security vulnerabilities.
9. **Computer Virus** is a program or piece of computer code that is installed or executed onto any computing device without the knowledge of the owner and runs against the owner's wishes. Most computer viruses will disrupt or alter the normal operation of the infected computer. Some computer viruses are destructive, permanently damaging data files or programs on a computer.
10. **Computing device** is an all-inclusive term referring to, but not limited to, desktop computer, laptop computer, Personal Digital Assistant (PDA), network, terminal, and any other computing device owned by the Institution.
11. **Custodian of an Information Technology Resource** is a person responsible for implementing owner-defined controls and access to an I.T. resource. (TAC 202.1(5))
12. **Distance Learning** is conducting live class sessions by holding discussions and delivering course content to geographically separated students in a fully interactive manner through the use of videoconferencing procedures, systems, and infrastructure.
13. A **Distance Learning Classroom** is a TTUHSC classroom equipped with a multi-media teaching podium, instructor video monitor, sound reinforcement system, student microphones, video cameras, VGA/video projector, projection screen, and associated items, connected to the TTUHSC network infrastructure for the purpose of conducting distance learning class sessions.
14. **e-Commerce** is a special web application that allows users to make online payments or purchases with a credit card.
15. **Firewalls** are security systems which control and restrict both network connectivity and network services, usually from the Internet. Firewalls establish a perimeter where access controls are enforced. Connectivity reflects which systems can exchange information. A service, sometimes called an application, refers to the way information flows through a firewall. Examples of services include FTP (file transfer protocol) and HTTP (web services).

16. **Host** is a hardware device that is connected to the TTUHSC network, and capable of transmitting and receiving data using Transmission Control Protocol/Internet Protocol (TCP/IP), the suite of communications transmission formats used to connect hosts on the Internet. Examples of hosts are personal computers, servers, printers, scanners, and network equipment.
17. **Information Security Officer (ISO)** is the individual appointed by the president or their designee and is responsible for administering the Institutional information security program. Under the direction of the CIO, the Information Security Officer is TTUHSC's primary internal and external point of contact for all Information Technology security matters.
18. **Information Security Program** consists of the elements, structure, objectives and resources that provide information resource security for the Institution (TAC 202.1.8)
19. **Information Technology (I.T.) resources** include any and all hardware, software, and data used to create, store, process, and communicate information electronically as well as services to keep these resources current and operational.
20. **Information Technology Security Council (ITSC)** consists of representatives from each of the schools, and operational divisions; the CIO; the Associate Vice President of Technology Services; the Assistant Vice President of Information Services; the Information Technology Security Team; and the regional Computer Security Analysts. Each representative is appointed by executive management. The ITSC is responsible for insuring the Institutional security program aligns with Institutional business objectives.
21. **Information Technology Security (ITS) group** is newly formed within the I.T. Division and is comprised of the Information Security Officer and two Computer Security Analysts. Under the direction of the CIO, the ITS group is responsible for overseeing Institutional network security and computer virus protection activities.
22. **Interference** is the degradation of a communication signal, whether wired or wireless in origin, caused by electromagnetic radiation from another source. Such interference can distort, slow down, or completely eliminate the transmission of a communication signal, depending on the strength of the interference.
23. A **key public entry point** is defined as a web page that is specifically designed for members of the general public to access official Institution information. TTUHSC has designated the following as key public entry points:
 - the main Institutional home page (<http://www.ttuhs.edu>),
 - all regional campus home pages (<http://www.ttuhs.edu/amarillo/>, <http://www.ttuhs.edu/el Paso/>, <http://www.ttuhs.edu/odessa/>), and
 - all official schools and the health care system home pages.
24. A **Multi-media Teaching Podium** is the presentation device installed in each TTUHSC distance learning classroom, and containing a PC, digital tablet, document camera, computer screen, slide-to-video converter, VCR, user microphone, user control panel, and related network interface equipment.
25. **Network** is a system that transmits any combination of voice, video, and/or data between users. The network includes the network operating system in the client and server machines, the cables connecting them and all supporting hardware in between such as bridges, routers, multipoint control units, video codecs, and switches. In wireless systems, antennas, transmitters, and towers are also part of the network.

26. **Non-broadcast** refers to single site (non-TechLink) use of TTUHSC videoconferencing resources.
27. A **Notice of Disclaimer of Liability** is a statement repudiating the accuracy of the information contained on a web site and/or web page. A link to the Notice of Disclaimer of Liability must be included in the footer section of all key public entry points.
28. **Origination Site** refers to the TTUHSC distance learning classroom that is the controlling location in a videoconferencing session (usually the location where the instructor or presenter is physically present).
29. **Owner of an Information Technology Resource** is a person responsible: for a business function; and for determining controls and access to information resources supporting that business function. (TAC 202.1.10)
30. A **Regional Site Coordinator (RSC)** is the administrator of all local area networks (LAN) at each campus. The RSC is the contact person for all connectivity issues between the regional campus LAN's and the TTUHSC wide area network (WAN).
31. **Security** is defined as all measures to protect electronic hardware and software communication resources from unauthorized access and to preserve resource availability and integrity.
32. **Security Incident** is an event which results in unauthorized access, loss, disclosure, modification, disruption, or destruction of information resources whether accidental or deliberate. (TAC 202.1.14)
33. **Security Risk Analysis** is the process of identifying and documenting vulnerabilities and applicable threats to information resources. (TAC 202.1.15)
34. **Security Risk Assessment** is the process of evaluating the results of the risk analysis by projecting potential losses, assigning levels of risk, and recommending appropriate measures to remediate the risk. (TAC 202.1.16)
35. **Security Risk Management** are decisions to accept exposures or to reduce vulnerabilities to information resources. (TAC 202.1.17)
36. **Server** is a computer program that provides services, applications, and resources to computer users in the same, or another computer. A computer running a server program is frequently referred to as a server though it may also be running other client (and server) programs.
37. **TechLink** is all videoconferencing equipment, systems, infrastructure, and network used in distance learning, telemedicine, and general purpose videoconferencing at TTUHSC.
38. **Telemedicine** is the delivery of healthcare services to patients at distant locations through the use of videoconferencing procedures, systems, and infrastructure.
39. A **Telemedicine Consultation Facility** is a room equipped with a video camera, video monitor, videocassette player, and microphone, connected to the TTUHSC network infrastructure for the purpose of conducting telemedicine consultations and related videoconferencing activities.
40. An **Unauthorized Access Warning Banner** is a message informing the potential users of access restrictions to the system and is an important passive tool in assuring the security of TTUHSC computing system resources and the information contained therein.
41. **User** is an individual or automated application authorized to access an information resource in accordance with the owner-defined controls and access rules. (TAC 202.1.20)

42. **Videoconferencing Infrastructure** is defined as all network support equipment such as audio amplifiers, audio mixers, audio/video routers, CSU/DSUs, encoders, MCUs, PCs, software, touch panels, video codecs, video distribution amplifiers, video monitors, video quad mixers, video switchers, and similar devices installed in TTUHSC network control centers; and operated, maintained, and supported by the TTUHSC Information Technology Division for the purpose of providing distance learning, telemedicine, and general purpose video teleconferencing services to TTUHSC.
43. A **Videoconferencing Resource Reservation** is the confirmed allocation of videoconferencing resources to support a specific TechLink or non-broadcast event, or series of related events (such as recurring class sessions in a specific course).
44. A **Videoconferencing Resource Reservation Request** is an application by a user to schedule (or reserve) videoconferencing resources at TTUHSC.
45. A **Videoconferencing System** is defined as all interactive audio-visual equipment such as multi-media teaching podiums, video cameras, student microphones, video monitors, VGA/video projectors, and related items installed in TTUHSC distance learning classrooms, conference rooms, telemedicine consultation rooms, and similar facilities, and supported and maintained by the TTUHSC Information Technology Division.
46. **Virtual Private Network (VPN)** is one or more encrypted connections over a shared public network, typically over the Internet, which simulates the behavior of direct, local connections.
47. A **web page** is defined as any information that is displayed through web browsers. It is the basic building block of web sites and is identified by a unique Universal Resource Locator (URL).
48. A **web site** is several inter-related and cross-linked web pages designed to function as a collective unit.
49. **Wireless Infrastructure** includes wireless access points, antennas, cabling, power, and network hardware associated with the deployment of a wireless communications network. This is also referred to as Wireless Local Area Networking, or WLAN.