

Section VIII: Facilities Services, Safety, Info & Tech

Chapter 1: Environmental Health and Safety

Environmental Health and Safety Office (EH&S) is a campus risk management function that exists to develop, promote and maintain a safe, healthy learning and working environment for the students, faculty, staff and visitors of the University. EH&S operates within the Division of Oversight under the authority of the Executive Vice President and is responsible for environmental compliance, fire and physical safety, chemical hygiene, biological safety, radiation safety management, Workers' Compensation, safe Return to Work, and other loss prevention efforts.

1.1 Environmental Health and Safety Policies

1.1.1. It is the policy of the University to furnish a place of employment and learning that is as free as possible from recognized hazards that cause or are likely to cause harm or death of its faculty, staff, students, visitors and/or the surrounding community.

1.1.2. Administrators, faculty, staff and students share in this responsibility and are expected to ensure that their actions as well as activities under their control are conducted in a manner that presents the least possible hazard to themselves, other members of the University community, visitors, University property and/or the surrounding community.

1.1.3. The Director of EH&S is responsible for development of safety-related policy recommendations, implementation of procedural guidelines, and, through an ongoing audit and observation function, providing reasonable assurance to the President that the institution is in compliance with approved safety standards and policies. The Director is further empowered to take interim action to close, evacuate or bar entry to any area, space, classroom, laboratory or office and order the cessation of any activity on property own or controlled by the University which, in the opinion of the Director represents a possible danger to members of the University community or University property, including repeated violation or flagrant disregard of University safety policies.

1.1.4. University personnel shall comply with all applicable federal and state statutes, ordinances, rules and codes; generally accepted industrial safety standards; and University policies contained in EH&S procedural manuals which are incorporated by reference into this handbook and are available electronically at: <http://admin.utep.edu/Default.aspx?tabid=7393>.

1.2 Radiation Safety

EH&S is responsible for monitoring the safe use of radioisotopes at the University to ensure compliance with regulations governing use of radioactive sources, X-ray generating devices, and lasers. The University operates under Academic Radioactive Materials License #L-00159 issued by the Radiation Control Division of the Texas Department of State Health Services. An EH&S Radiation Safety Officer shall monitor all areas where radioactive materials are used to ensure regulatory requirements and conditions of University licensure are adhered to by departmental sub-licensees. All University employees seeking to utilize radioactive materials or radiation producing equipment must register with EH&S and receive appropriate mandatory training before use will be granted under the University license.

1.2.1 The EH&S Radiation Safety Officer monitors all areas where radioactive materials are used to ensure regulatory requirements and conditions of University licensure are adhered to by departmental sub-licensees. All University employees seeking to utilize radioactive materials or radiation producing equipment must register with EH&S and receive appropriate mandatory training before use will be granted under the University license.

1.3 Biological and Chemical Safety

EH&S is responsible for monitoring the safe use and disposal of chemical and biological agents at the University to ensure compliance with prudent laboratory practices, National Institutes of Health guidelines, requirements of the Center for Disease Control and U. S. Department of Homeland Security, and the Texas Health and Safety Code. Hazardous chemical training and biological safety training are required of all University personnel who will use or encounter these materials during the course of their work. All University personnel seeking to utilize hazardous chemicals and/or biological agents must register and receive appropriate mandatory training from EH&S. Principal investigators are further responsible for insuring that all personnel under their direction have received appropriate training to address the hazards of specific chemicals or biological materials used in their research. Where research protocols will involve infectious agents or recombinant DNA, researchers shall seek pre-approval and continuing approval of the proposed research through submission of specific information for the consideration of the Institutional Biosafety Committee (IBC). IBC procedures may be found in the Biosafety Manual published at the EH&S procedural manuals website.

1.4 Physical Safety and Loss Prevention

The University's Physical Safety program is designed to ensure that all reasonable steps are taken to preserve life and property from exposures to fire and other hazards, and to take measures aimed at loss prevention to include not only corrective actions but also to educate the campus community in its role to preserve life and property. The program is meant to serve as a helpful resource for managers and supervisors who must carry out specific procedures related to loss prevention.

1.4.1. EH&S monitors University operations and facilities campus-wide to ensure continuity of physical safety and the functionality of building safety system (such as fire protection and detection systems) through a program of regular facility inspections and provision of appropriate loss prevention and emergency preparedness safety training for the University community.

1.5 Occupational Safety and Health

The University recognizes the Occupational Safety and Health (OSHA) national standards and uses its provisions as an important guide in establishing and implementing institutional policies as contained in [EH&S procedural manuals](#). The University also complies with provisions of the Texas Health and Safety Code, which adopts many of the basic OSHA principles into State law. EH&S provides job safety training and monitors compliance with the policies, manuals and rules to assure adequate and appropriate care is given to protect University employees. All records regarding employee training and workplace inspections are maintained by EH&S.

1.5.1. EH&S supports research endeavors and other at risk functions of the campus through administration of a program of occupational risk assessment and health monitoring where the routine duties of employees are found to present an increased risk for occupational illness or disease.

1.6 Environmental Compliance

EH&S is responsible for monitoring compliance with all applicable federal and state environmental laws including the application and receipt of required permits, and the gathering and reporting of all regulatory required data.

1.6.1. EH&S represents the University before all regulatory agencies having environmental authority. This includes but is not limited to all matters pertaining to hazardous waste management, asbestos project monitoring and abatement, air quality permitting, storm water management, annual hazardous wastes summaries, Universal Waste records, fuel usage reports, air emission calculations and reports, and other environmental data as may be required by law or governmental regulations.

1.7 Workers' Compensation Insurance

The University's Workers' Compensation Insurance (WCI) program is a state regulated insurance plan that covers medical treatment and rehabilitation for work related injuries and illnesses. WCI also pays a portion of income lost while an employee is away from work recovering.

1.7.1. EH&S is responsible for all employer functions related to the University's Workers' Compensation program, which includes providing assistance to employees who experience a work related injury or illness, electronic reporting of claims to the insurance carrier, and return to work. EH&S also ensures timely compliance by the University of the Texas Department of Insurance, Workers' Compensation Insurance rules and regulations.

1.7.2. The University's Return to Work (RTW) program provides opportunities for an employee who is injured on the job to return to work at full duty. If the injured worker is not physically capable of returning to full duty, the RTW program provides opportunities to perform regular job duties with modifications or, when available, to perform alternate temporary work that meets the injured worker's physical capabilities. The program is designed to encourage and actively assist injured workers in the successful return to work.

Chapter 2: Institutional Building Advisory Committee

As stated in the Regents' [Rules and Regulations](#), Part II, Chapter VIII, Section 2., at each of the component institutions there shall be an Institutional Building Advisory Committee. The purpose of the Institutional Building Advisory Committee is to advise the President and the Board of Regents (through the President) on the physical development of the campus and its facilities.

2.1 Committee Duties

To review and make recommendations periodically concerning additions and deletions to the University master plan for land acquisitions, new construction, major remodeling or demolition of existing facilities;

To review specific requests for new facilities and/or requests for major remodeling of buildings and to recommend appropriate action on these requests to the President, including priorities for recommended projects;

To consider and make recommendations for major reallocation of space use in existing University facilities.

2.2 Committee Membership

Two faculty members appointed by the President for two (2) year terms.

The Dean of Student Affairs.

The Director of the Facilities Services.

The Chair of the University Parking and Traffic Committee.

The Chair of the Faculty Senate Physical Facilities Committee or Faculty Senate designated representative.

An Assistant to the President or other designated representative of the President.

The President of the Student Association.

The Provost. (Ex-Officio)

The Executive Vice Chancellor for Business Affairs. (Ex-Officio)

The Committee Chair shall be the Vice President for Business Affairs.

The Committee shall meet at least once per academic year and at such other times as called by the President or the Chair.

The Committee may establish such sub-committees as required for the orderly conduct of its duties. Such sub-committees may contain members from outside the full Committee.

Chapter 3: Institutional Insurance(s)

The University is exposed to various risks. Depending on the type of risk, the University may purchase insurance to handle potential financial losses. A description of some of the insurance policies purchased by the University is given below. For further information about University insurance policies, contact the Office of the Vice President for Business Affairs.

3.1 Automobile Insurance

Automobile Liability

The automobile insurance policy provides liability coverage for those automobiles owned and operated by the University. (The proof of insurance coverage certificate is not required to be carried in University owned vehicles.) The policy currently carries a \$2,500 deductible per accident. Policy limits are:

Bodily Injury - \$250,000 each person;
Bodily Injury - \$500,000 each accident;
Property Damage - \$100,000 each accident.

Hired/Non-Owned

This policy provides liability coverage (secondary coverage to an individual's personal policy) for employees using their personal vehicle for business use. This policy also provides liability, comprehensive and collision coverage on short-term rental vehicles, including those rented by employees outside the System rental car agreement in force. This policy does not provide coverage for damage to an employee's personal vehicle or personal effects.

Policy limits are:

Bodily Injury - \$250,000 each person;
Bodily Injury - \$500,000 each accident;
Property Damage - \$100,000 each occurrence.

(Please note there is a \$2,500 deductible on liability, \$0 deductible on the comprehensive and \$500 on the collision coverage with a maximum physical damage limit of \$75,000.).

Mexico Coverage

Mexico coverage for automobiles is provided on an as-needed basis. Coverage is to be secured through the Vice President for Business Affairs Office in order to ensure sufficient and consistent coverage.

3.2 Boiler and Machinery Coverage

Boiler and machinery coverage is provided under the Comprehensive Property Protection Plan (CPPP). Boiler and Machinery coverage will pay for direct damage to "covered" equipment caused by a "breakdown". For more information, contact the Office of the Vice President for Business Affairs.

3.3 Fidelity and Crime Policy

This policy covers losses resulting from employee dishonesty or dishonest acts committed by non-employees. The policy carries a \$100,000 loss retention per occurrence. Coverage amounts are listed below:

Coverage	Limit
Employee Theft or Forgery	\$3,000,000
Theft, Destruction, Disappearance by a third party.	\$3,000,000
Forgery or Alteration by a third party	\$3,000,000
Computer Fraud by a third party	\$3,000,000
Funds Transfer Fraud by a third party.	\$3,000,000
Money Orders & Counterfeit Currency Fraud by a third party.	\$250,000
Credit Card Fraud	\$250,000

3.4 Comprehensive Property Protection Plan

This plan is a combination of self-insurance and commercial property insurance coverage. It provides coverage for all real and business personal property of the University. For further information, contact the Office of the Vice President for Business Affairs.

3.5 Endowment Property

This policy provides property and liability coverage for certain properties donated to or acquired by the University, depending on the conveyance agreement. It also covers property "leased" by the University, which may require such coverage(s) under the lease agreement.

3.6 Equipment Floater Coverage - Worldwide

The policy provides coverage for equipment owned, borrowed or leased by the University and that are scheduled on the policy. The policy provides worldwide coverage except for North Korea, Libya, Iran, Iraq, Afghanistan, Syria, Liberia, and Cuba, however, this policy excludes coverage for ocean cargo shipments. U. T. System Office of Risk Management should be consulted prior to departure if equipment will be leaving the Continental United States so that the appropriate ocean cargo insurance can be purchased.

Limits of Insurance:

\$20,000,000 any one occurrence, not to exceed;

\$ 1,500,000 on any one item

\$ 5,000,000 flood annual aggregate

\$ 5,000,000 earthquake outside the state of California annual aggregate
\$ 1,500,000 any one occurrence while in transit
\$ 1,500,000 new acquisitions reported within thirty (30) days
\$ 1,500,000 any one occurrence as to property loaned to insured on a temporary basis.
\$ 500,000 any one occurrence as to property loaned/rented/leased to others
\$ 500,000 any one occurrence as to property while waterborne, underwater, or over the side in any one watercraft
\$ 500,000 any one occurrence as to flood, earthquake, and wind outside the Continental United States and Canada
\$ 100,000 any one occurrence as to mechanical breakdown

Deductibles:

\$ 2,500 per occurrence, except \$1,500 as to Laptop Computers; and
\$ 100 as to Oximeters
\$25,000 per occurrence as to Flood
\$25,000 per occurrence as to Earthquake

3.7 Fine Arts

Fine Arts insurance provides coverage for University owned fine arts and for fine arts loaned to the University against all risks of physical loss or damage from any external cause subject to policy exclusions. This policy covers paintings, etchings, drawings, rare books, manuscripts, rugs, tapestries, statuary, other bona fide works of art or rarity, historic value or artistic merit. Coverage is also provided while on exhibition and while in transit within and between the United State, the District of Columbia and the Provinces of Canada.

Limit of Liability: \$1,146,000

Deductible: \$500 for owned art; \$5,000 for outdoor sculptures

3.8 Sports Special Events - General Liability Policy

This policy provides spectator liability coverage for NCAA sponsored and similar events at the University with a limit of \$1,000,000. Institutions are to notify the Vice President for Business Affairs Office at least two weeks prior to the event's date in order to acquire coverage. This is a "reporting" policy and coverage is provided only when the U.T. System Office of Risk Management is notified prior to event dates.

3.9 Camp Insurance Program

This program provides a combination of general liability and accident coverage to any University owned and operated academic and sports camps. This is a "reporting" policy and coverage is provided only when the U.T. System Office of Risk Management is notified prior to the camp date.

3.10 Insurance Purchasing Rules

According to the Board of Regents' Rules, component institutions can solicit bids or ask U.T. System Office of Risk Management to bid the insurance policy. All policies must be approved by the Director of ORM or Executive Vice Chancellor for Business Affairs.

3.11 Policy Review

This chapter on institutional insurance coverage is for information purposes only and is intended only to serve as an overview of some of the University's insurance policies. The actual coverage terms and

conditions will be determined by the applicable language in the insurance policies. Revisions to these policies will be made as needed to comply with changes in law or regulation, or to enhance their effectiveness. Contact the Office of the Vice President for Business Affairs with any insurance questions

Chapter 4: Information Computing and Web Policy

4.1 Introduction

The [Rules and Regulations](#) governing information/computing policies for the University of Texas at El Paso are intended to supplement existing policies published by the Texas Department of Information Resources, the University of Texas System, as well as reinforcing the Texas Computer Crimes Law and laws governing the use or misuse of state property.

It is imperative that all users of the University's information/computing and information resources realize how much these resources require responsible behavior from all users. We are all responsible for the well-being of the information/computing, network, and information resources we use. It is the intent of these policies and procedures to provide general guidance in the proper use of these resources for optimal use.

We acknowledge our commitment to promote the open exchange of ideas; however, an open, cooperative information/computing network can be vulnerable to abuse or misuse. As more and more schools, colleges, universities, businesses, government agencies, and other enterprises become attached to the world-wide information/computing and information networks, it is critical that we ensure that our students, faculty, and staff are well aware of our individual and institutional responsibilities in the use of state resources.

4.2 Purpose

The University of Texas at El Paso recognizes University information/computing resources as valuable state assets and will manage these resources accordingly. Information/computing resources include all computer and telecommunication hardware, software, and networks owned, leased, or operated by the University, and the data or information stored therein. The following policies establish the governing philosophy for the use of these resources by students, faculty, staff, and other specifically authorized individuals or entities, to ensure compliance with State laws and regulations regarding the use and security of University information/computing resources, and to provide the maximum benefit of these resources to the University community.

These policies augment and incorporate by reference the following:

The University of Texas System Business Procedure Memorandum 53-02-96.

The Texas Department of Information Resource, Information Security and Risk Management Policy, Standards and Guidelines. (Texas Administrative Code, 1TAC201.13(b).

The Information Resources Management Act. (Texas Government Code, Section 2054.001 et seq.)

The Texas Computer Crime Statute (Texas Penal Code, Section 33.02).

All use of University information/computing resources must comply with applicable Federal and State laws as well as U. T. System and University regulations as they relate to the proper use of State property; the observance of intellectual property rights; the protection of information and computing resources from damage, disruption, or misuse; and requirements concerning content. All users, whether student, employee, or other authorized individuals, are required to be aware of, abide by, and enforce the provisions of these policies.

4.3 Statement of General Policy

In support of its mission of teaching, research, and public service, the University of Texas at El Paso provides access to information/computing resources for students, faculty, and staff, to the extent permitted by the financial resources of the University as reflected within established institutional priorities.

The access granted students, faculty and staff to the University's information/ computing resources is a privilege, not a right. The University may limit, restrict, deny or extend access to its information/computing resources in any manner that may be required to protect information held confidential by law, to protect the integrity of the contents of data files and to provide for orderly and efficient use of information/computing resources.

Authorized users of University Information/Computing resources are:

1. University students who are limited to the use of those information/computing resources specifically assigned to serve educational purposes.
2. University employees who are provided access to those information/computing resources required for the performance of their duties in the conduct of official business. Access to any particular administrative data file must be based on an employee's "need to know" as established by his or her official duties and reflected in the advance provision of specific authorization codes, passwords or other access enabling means to the employee.
3. Non-University affiliated individuals or entities may not use University information/computing resources except after written agreement for purposes related to the University's missions.

All users of University-owned, leased or controlled information/computing systems must act responsibly, respect the rights of other users, protect the physical facilities and equipment, and observe all pertinent license and contractual agreements affecting the use of systems, hardware or software.

Information/computing facilities and accounts are to be used only for University- related activities by the person to whom they are assigned. The University's information/computing resources may not be used for the conduct, advertisement, promotion, or any form of solicitation, on behalf of any non-University operated business, corporation, organization, enterprise or activity, whether profit or non-profit in nature, nor may University resources be used by individuals for personal benefit or private gain, including the conduct of consulting services by faculty or staff.

Because all files created or maintained using the University's information/computing resources are property of the University; it must be understood that the University can convey no expectation of privacy or confidentiality to a user. While general access to specific files can be limited or controlled where appropriate for legitimate business reasons, authorized University officials can enter and examine the contents of all files maintained on university-owned equipment. All user files are further subject to external review and possible public release resulting from a search warrant or subpoena issued and served pursuant to law, or a valid request under the Texas Public Information Act.

4.4 WEB and Internet Access and Use

The University of Texas at El Paso recognizes the value and potential of information published on the Internet via the World Wide Web and encourages all faculty, staff, and students to develop innovative uses of web technologies in pursuit of the University's mission. To achieve this purpose, the University owns and operates web servers to facilitate the educational process and enhance research and publication by University faculty, staff and students.

Because the University recognizes the value of the Internet as a resource for information and communication, students and employees may make incidental use of University resources to access the web for co-curricular or personal purposes provided they abide by the general policies and procedures governing use of information/computing resources and there is no direct cost to the University attributable to such incidental use.

4.4.1 Web Sites

University Web sites are segregated into two distinct sets: official web pages, and individual web pages. Because the University's web sites support diverse purposes and diverse constituencies, Webmasters, Site Owners, and personal page creators are accorded wide discretion for the selection of content and for establishing reasonable and appropriate policies applicable to their sites. However, because anything placed on the internet from the University is easily identified as originating from the University network, some readers may assume that publications are somehow sponsored by the University. Even with disclaimers, the University is represented by its students, faculty and staff, and appropriate language, behavior and style is warranted.

4.4.2 Official Web Pages

Official web pages are provided exclusively for the dissemination of official policies and procedures; the description of budgeted University offices and departments, their services, programs and activities, including identification of associated faculty or staff members; and the provision of operational instructions or information necessary to assist students, employees, and entities with whom the University conducts business.

Official sites are authorized for administrative divisions and offices; academic departments; grant programs and research centers or activities authorized by the Office of Research and Sponsored Projects; and other activity or informational centers authorized by the President or a Vice President. The supervising administrative officer for each unit that publishes an official web site is responsible for the establishment, security, and content of all pages within the site.

The primary University Web Server (<http://www.utep.edu>) is administered by the staff of the Networking and Telecommunication Services Department. Administrative access to the web server is restricted to Networking and Telecommunication staff and their designees. All file owners on the server should be aware that the system administrators are co-owners of all files.

While respecting the users' confidentiality and privacy, the University reserves the right to examine all computer files. The University reserves this right to enforce its policies regarding acceptable use of University resources; to prevent the posting of proprietary or copyrighted material; to safeguard the integrity of computers, networks, and data either at the University or elsewhere; and to protect the University against seriously damaging consequences.

4.4.3 Individual Web Pages

All faculty, staff, and students are provided space for personal web pages on the server. Individual web pages are the responsibility of the page creator and do not reflect the opinions, positions, policies, or procedures of the University. Anonymous web pages are prohibited, and all individual web pages must prominently display the name(s) of the creators who assume full legal and ethical responsibility for the content thereof.

4.4.4 Web Accounts

User accounts on the primary University web server <http://www.utep.edu> are available to: academic colleges, academic departments, administrative departments, official student organizations (as determined by the Dean of Students), and official research centers or groups (as determined by the Office of Research and Sponsored Projects, an academic Dean, or an academic Department Chair).

The administrative authority responsible for the department or group is designated as the Site Owner and is responsible for securing access to the account and for all material posted to the account. Site Owners are expected to control access to the account and share the password sparingly and to modify the password from time to time.

Acceptable Use

1. To facilitate communication and dissemination of information to University faculty, staff, and students regarding University services and programs.
2. To facilitate communication with current and prospective business partners for the daily operation of University business.
3. To advertise and promote University programs and services to prospective students, professional colleagues, and the general population.
4. To support professional societies, government advisory, or standard activities related to the users' professional/vocational discipline.
5. To apply for or administer grants or contracts for work-related applications.
6. To announce products or services for use within the scope of University business, but not for commercial advertising of any kind.
7. For official sites, any other communications or activities in direct support of University related research, instruction, learning, dissemination of scholarly information, and administrative activities.
8. For personal sites, any other communications or activities that are not in violation of this or any other University policy, or applicable federal, state or local law.

Unacceptable Use

All Internet and Web use is subject to the general policies governing use of University's information/computing regulations. In addition, the following uses or contents are expressly forbidden on any University web page, official or individual:

1. Publishing or linking to any material prohibited by law or University regulations, material that violates the terms of any University license or contract, or uses copyrighted material without required permission.
2. Publishing or linking to legally restricted or confidential material.
3. Publishing or linking to material that is obscene, libelous, physically threatening or otherwise in violation of standards for University publications.
4. Publishing or linking to material that intentionally or negligently may lead to damage to a University or other computer system;
5. Using the University seal, logos or other registered University marks without the review and

approval of the University Communication Office. Such approval will not be granted for individual web pages.

4.5 E-Mail Use

The University recognizes the institutional benefit of the provision of electronic mail services and encourages all students and employees to obtain the necessary accounts and/or passwords to enable them to use this communication service.

All e-mail use is subject to the general policies governing use of University information/computing resources. In addition, the following uses or activities are expressly prohibited:

1. Transmission, display, printing or storage of any material prohibited by law or University regulations;
2. Unauthorized transmission, display, printing or storage of legally restricted or confidential material.
3. Transmission, display, printing or storage of material that is obscene, libelous, or physically threatening;
4. Transmission, display, printing or storage of material which advertises, promotes or otherwise solicits on behalf of any non-University business, corporation, organization, enterprise or activity or which contributes to the conduct of business by such entities. This includes the conduct of private consulting services by faculty or staff employees of the University.
5. Transmission, display, printing, or storage of any material through the fraudulent use of another person's password. Any use of another person's password is prohibited.
6. Transmission, display, printing or storage of chain letters, and other forms of mass mailings or any use that may disrupt or delay the timely and orderly provision of e-mail services at the University. The System Administrator only upon the approval of the President or a Vice President of the University may place general broadcast messages on the e-mail system.
7. The content, maintenance, disposition or retention of e-mail messages is the responsibility of the person to whom the e-mail account or address is assigned. E-mail that conducts official business must be maintained for future reference in accordance with the University's Records Retention policies, which reflect the requirements of state law. In order to obtain optimum efficiency and service, the System Administrator will delete e-mail messages older than 2 weeks that have been accessed from central file servers. E-mail messages requiring retention beyond this time limit should be downloaded to disks or printed for storage by each user.

4.6 Information Resources Security Policy

Please refer to the next section

4.6.1 Introduction and Overview

The University relies on Information Resources to support its mission of achieving excellence in undergraduate and graduate education, research, and public service. These resources are critical to the University's academic, research, and business operations. The Information Resources policy, hereafter referred to as the policy, informs all who use the University's Information Resources of their responsibilities in securing these valuable assets. Authority for the policy originates from federal and

state laws and regulations. The Vice President for Institutional Advancement is charged with its implementation.

The policy applies to all students, faculty, staff, visitors, or others who:

1. Store information on University computers;
2. Use the University's Information Resources, whether affiliated with the University or not;
3. Have computing equipment connected to the University's Information Resources, or Access the University's information.

4.6.2 Compliance and Enforcement

Compliance with the terms of the policy is required. When investigations of security breaches or misuse result in credible evidence of violations of University policies or criminal activity, those responsible will be subject to removal of access to resources, disciplinary actions, and possible criminal prosecution. If an Information Resource that is attached to the University's computing infrastructure is found to be insecure or negatively impacts the University's infrastructure, the University may take measures to protect the security and ensure the continued availability of the University's infrastructure. This shall include requiring the Information Resource be removed from service until a proper resolution has occurred.

4.6.3 Purpose

The policy establishes a framework for securing the University's Information Resources, in compliance with University and state information security standards, applicable state and federal laws, University rules, and exercise of due care.

As security threats evolve and increase, the University and every individual Information Resource user must protect the University's infrastructure, attached systems, and data, including all confidential, sensitive, and private information processed, stored on, or transmitted by these resources. The policy and other supporting documents are designed to preserve the availability, utility, integrity, authenticity, confidentiality, and possession of the University's Information Resources and guard them from threats such as:

1. accidental or intentional destruction,
2. interference with use,
3. falsification, concealment or misrepresentation of identity or\ authorization, misuse or abuse,
4. threats against persons or property,
5. unauthorized or wrongful access,
6. unauthorized modification or observation,
7. unauthorized copying, data retrieval, or replacement,
8. repudiation of authentic transactions, and unauthorized disclosure.

4.6.4 Responsibilities of Those Using the University's Information Resources

Everyone who uses Information Resources at the University is required to:

1. Read and acknowledge this and other applicable information security policies.
2. Be aware of confidential, sensitive, or private information on the resources they control and institute appropriate security procedures and controls.
3. Manage their Information Resources in a way that poses no internal or external security or operational hazard.
4. Stay informed of current threats that may affect Information Resources they own or manage.
5. Cooperate promptly with University staff in correcting problems involving Information Resources under their control.
6. Report Information Resource security incidents to the custodian or owner of the device or information affected. When the custodian or owner cannot be reached, contact the Information Security Office.

4.6.5 Specific Roles and Responsibilities

Please refer to the next section

4.6.5.1 Executive Officer

The President, or a designated representative, shall review and approve ownership of Information Resources and their associated responsibilities.

4.6.5.2 Owners of Information Resources

An owner of Information Resources is a person who is ultimately responsible for determining controls and access to the Information Resource. Owners may include deans, department heads, directors, researchers, or technology managers.

Owners of Information Resources shall:

1. Approve access and assign custody for Information Resources.
2. Grant sufficient authority to implement security controls.
3. Ensure that assigned custodians receive appropriate training or instruction to fulfill security responsibilities.
4. Include security considerations as an integral part of acquisition and budgeting. This includes grant proposals submitted either by individuals or University units.
5. Ensure implementation of security controls consistent with University rules and security standards, and state and federal laws.

4.6.5.3 Custodians of Information Resources

A custodian is a person who is responsible for implementing the security controls and access defined by the Information Resource's owner. Custodians may include technology managers, system or network administrators, or other designated individuals.

Custodians of Information Resources shall:

1. Implement approved controls, standards, and best practices on their assigned resources.
2. Assist owners in evaluating security controls.
3. Monitor access to the resources they manage to maintain security, operational, and privacy requirements. Monitoring shall be performed in accordance with University rules and state and federal laws.
4. Take all reasonable measures to protect Information Resources, which may include blocking, suspending, or revoking access to University Information Resources from sources that pose an immediate threat of harm or interfere with normal operations.
5. Report Information Resource security incidents to the Information Security Office.
6. Ensure that security considerations are examined when evaluating potential Information Resource purchases or services.
7. Attain and maintain security knowledge and expertise appropriate to the scope of assigned responsibilities.
8. Maintain necessary records on Information Resources under their management and control.

4.6.5.4 The Information Security Officer

The Information Security Officer (ISO) serves as Director of the Information Security Office.

The ISO shall:

1. Protect the security and ensure the continued availability of the University's Information Resources in accordance with University rules and state and federal laws. This shall include authorization to require that Information Resources that are found to be insecure or that negatively impact the University's infrastructure be removed from service until a proper resolution has occurred. The ISO will notify the owner and appropriate authorities whenever a resource must be removed from service.
2. Document and maintain a comprehensive information security program for the University.
3. Develop and maintain an institutional information security risk management program.
4. Provide direction for University-wide Information Resources security policies.
5. Establish and disseminate procedures and practices to facilitate owner and custodian compliance with security rules, policies, and laws.
6. Investigate reports of security breaches or misuse using standards of privacy and confidentiality required by law and University policy.
7. Assemble and coordinate Information Resources incident response teams, provide investigative assistance, and work with resource owners and custodians to resolve incidents.
8. Disseminate security information alerts, recommended practices, and periodic incident summary reports.

9. Promote University-wide security awareness and education.

10. Propose and participate in standing committees and councils related to University Information Resources security issues.

11. Assure that requests by law enforcement agencies, requests for information protected by state and federal law, and public information requests received by the Information Security Office are handled within established University policies and procedures.

12. Submit official Information Resources security reports as required by state or federal agencies.

4.6.6 Departmental Policies

Departments and units may adopt additional security policies and procedures so long as they meet the minimum standards of the policy and do not conflict with the policy, applicable laws, or other University rules. Departmental security policies that predate the policy's adoption shall be revised to comply with its provisions.

4.6.7 Monitoring

Use of University Information Resources is subject to security testing and monitoring as permitted by applicable laws and policies.

4.6.8 Review

The policy will be reviewed biennially and updated as required by the Vice President of Institutional Advancement or his designee.

4.6.9 Glossary

Affiliated: Those closely associated with the University, e.g., students, faculty, and staff.

Authenticity: Validity, conformance, and genuineness of Information or Resources.

Availability: Usability of information or a resource for a purpose when it is needed.

Confidential Information: Information that is exempted from disclosure requirements under the provisions of applicable state or federal law, e.g., the Texas Public Information Act.

Confidentiality: Limited observation and disclosure of knowledge.

Control/Security Control: Any action, device, policy, procedure, technique, or other measure that improves security.

Data: a representation of information, knowledge, facts, concepts, or instructions that is being prepared or has been prepared in a formalized manner and is intended to be stored or processed, is being stored or processed, or has been stored or processed in a computer. Data may be embodied in any form, including but not limited to computer printouts, magnetic storage media, laser storage media, and punch-cards, or may be stored internally in the memory of the computer.

Disclosure: To divulge, reveal, make known or report knowledge to others either inadvertently or intentionally.

Due care: The degree of care established or expected by the University that should ordinarily be used by reasonable and prudent persons in fulfilling their duties and responsibilities.

Endangerment: To expose information or resources to harm or danger by not applying sufficient protection either through failure to implement controls or by circumventing or disabling controls.

Hardware: Tangible objects, such as disk drives, display screens, printers, or physical components.

Immediate Threat of Harm: A clear and present danger that, without prompt intervention, is likely to result in detriment or damage to Information Resources.

Integrity: Completeness, wholeness, and readability for information, soundness for a resource and quality being unchanged from a previous state.

Information Resources: The procedures, equipment, data, and software that are employed, designed, built, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information, and associated personnel including consultants and contractors. (Adapted from Tex. Government Code, Section 2054.003.) The term "Information Resources is not limited to devices physically located on campus, but include all that are used to access University Information Resources from any location."

Possession: The holding, control, and ability to use information or resources.

Private Information: Personal information that belongs to or affects an individual, which may or may not be protected from disclosure by law.

Repudiation: Denial or refusal to acknowledge or accept an act, transaction, or information as true, after having done so previously.

Security: Techniques for assuring the availability, utility, integrity, authenticity, confidentiality, and possession of Information Resources.

Security Incident: An event that results in unauthorized access, loss, disclosure, modification, disruption, or destruction of Information Resources, whether accidental or deliberate.

Sensitive Information: Institutional information maintained by the University that requires special precautions to assure its accuracy and integrity by utilizing error checking, verification procedures and/or access control to protect it from unauthorized modification or deletion.

Software: A set of computer programs, procedures, and associated documentation concerned with the operation of a data processing system; e.g., compilers, library routines, manuals, and circuit diagrams. Information (generally copyrightable) that may provide instructions for computers; data for documentation; and voice, video, and music for entertainment or education.

Utility: Usefulness of information or a resource for a purpose.

Appendix

The following minimum security policies and procedures for Information Resources can be found in the comprehensive Information Resources Policy at <http://www.utep.edu/infosec/manual.htm>:

Acceptable Encryption Policy
Acceptable Use Policy

Administrative/special Access Policy
Analog/ISDN Line Security Policy
Audit Policy
Change Management Policy
Database (DB) Credentials Policy
Dial-In Access Policy
Incident Management Policy
Intrusion Detection Policy
Network Configuration Policy
Password Policy
Physical Access policy
Portable Computing Policy
Privacy Policy
Risk Assessment Policy
Security Monitoring Policy
Sever Hardening Policy
Server Security Policy
Vendor Access Policy
Virtual Private Network (VPN) Policy
Virus Protection Policy
Wireless Communication Policy
E-Mail Procedures
Personnel Procedures
Web and Internet Access Procedures

4.7 Policy Enforcement

Violators of these policies may be subject to prosecution under applicable criminal or civil laws and/or to disciplinary action under applicable University regulations.

When a minor violation of this policy is detected, depending on the nature of the violation, the suspected violator may be notified by a computing system administrator or other appropriate University official and asked to remedy the situation, if such action is appropriate. If a reasonable resolution to the incident is not readily attainable, or in the case of more serious violations, further administrative action will be pursued by the appropriate authority. This procedure may result in:

1. the temporary or permanent loss of access to information and computing resources for the offending individual;
2. any other penalty deemed appropriate by a University disciplinary authority upon a finding or admission of guilt following normally afforded due process procedures;
3. criminal prosecution; or
4. any combination of the above.

Policy violations by students are handled by the Dean of Students in accordance with University of Texas at El Paso student disciplinary policies. Policy violations by faculty or other employees with academic appointments will be referred to the Vice President of Academic Affairs for appropriate personnel action. Policy violations by all other University employees will be reported to the appropriate Vice President or other supervising administrative officer for appropriate personnel action.

It is a crime to make unauthorized use of protected computer systems or data files on computers, or to make intentionally harmful use of such computers or data files. The seriousness of such a crime ranges

from Class B misdemeanor to third-degree felony. The University will prosecute all cases of unauthorized access to, or intentional damage or misuse of, University information/computing resources

Chapter 5: Fleet Management Plan

5.1 Vehicle Fleet Management Plan

House Bill 3125, 76th Legislature, mandates the Office of Vehicle Fleet Management (OVFM) of the General Services Commission (GSC), as directed by the State Council on Competitive Government (CCG), to develop a management plan for the state's fleet. This plan is to provide detailed recommendations for improving administration and operation of the state's vehicle fleet.

The State Vehicle Fleet Management Plan (the plan) addresses state agencies to include institutions of higher education and provides additional direction to implement the provisions of the bill. UTEP will strive comply with provisions of HB 3125.

5.2 Vehicle Assignment and Use

Motor vehicles owned by the University will be used solely for official business. Official business is defined as use that supports and provides a direct benefit to this University.

Motor Pool - The University maintains a portion of its fleet in a Motor Pool for use by University faculty/staff on official University business.

Vehicle / Field Assignment - Vehicles purchased with state appropriated funds, may be assigned to field employees providing specific criteria is met. The vehicle must be utilized to serve a mission critical function for an approved activity. Annual utilization must meet the minimum use criteria established by the "The Plan". UTEP does not assign vehicles to individual Administrative or Executive employees.

Vehicle / Departmental Assignment - Vehicles purchased with state funds and assigned to service departments on a permanent basis, must meet mission critical and specific use criteria. Departmental assigned vehicles are generally assigned to provide on campus service needs, i.e. (plant maintenance, grounds, electric, plumbing, carpentry, paint, mail service, etc.)

5.3 Vehicle Replacement

The guidelines adapted by the University provide minimum replacement goals for routine vehicle replacement. Attainment of these goals should minimize fleet capital and operating costs. In general, most vehicles should be replaced when they reach 6 years (72 months) of service or 100,000 miles, whichever comes first. However, there may be circumstances in which vehicles may be replaced sooner (such as excessive maintenance or repair costs) or retained longer (such as unusually low maintenance costs). We will utilize the table in HB-3125 that details replacement goals for different types of vehicles and vehicle uses as a guide for vehicle replacement recommendations.

Specialized equipment, such as heavy construction equipment, may not fall under any of the above categories. Such equipment may be considered for replacement according to other criteria, such as hours in service.

5.4 Fleet Fueling Policy

The University utilizes the statewide contract with Voyager for retail fuel dispensing services. Fuel cards are issued to specific vehicles. The Physical Plant maintains two regular unleaded fuel pumps and one

diesel fuel pump on campus. Unless specifically prohibited by manufacturer warranty or recommendations, all state vehicles operating on gasoline shall use regular unleaded gasoline.

5.4.1 Use of Alternative Fuels

Vehicles capable of using alternative fuels will use them exclusively except in certain cases specified in Title 1, Texas Administrative Code, Chapter 125, Section 125.69. Exceptions are:

- a. where and when the alternative fuel is not available;
- b. the range of the alternative fuel is insufficient to complete a round trip, in which case the alternative fuel shall be used until exhausted, with conventional gasoline or diesel fuel used only to complete the trip or until the alternative fuel is available;
- c. when the alternative fuel costs more than conventional gasoline or diesel;
- d. when conversion equipment is not working or is unsafe to operate, in which case timely repairs or inspections shall be made so that the vehicle may continue to operate on the alternative fuel; and
- e. when operating exclusively on an alternative fuel is contrary to the vehicle manufacturer or alternative fuel conversion equipment vendor recommendations.

5.4.2 Refueling at Self-Service Islands or Central Fueling Facilities Only

University employees will use self-service islands when refueling at retail fueling stations.

5.5 Sale of Excess Vehicles

The Fleet Operations Manager will determine when a vehicle is no longer practicable for use and declare the vehicle as surplus. Utilizing established State guidelines, the Materials Management Department will offer the excess vehicle together with other University surplus for sale to the highest bidder. Proceeds from the sale will be deposited to a designated University account.

5.6 Alternative Vehicle Use Option

Where cost savings are identified and appropriate approvals are secured, employees can utilize personal vehicles and apply for reimbursement through the appropriate channels.

5.7 Data Collection and Agency Reporting

The University of Texas at El Paso currently utilizes the "e-track" software to provide GSC information about the University's fleet.

Chapter 6: Naming of Buildings and Other Facilities

The naming of buildings and other facilities, including laboratories, classrooms, seminar rooms, lounges, galleries, and other campus areas, requires specific approval of the Board of Regents of the University of Texas System. As a general practice, University building names shall reflect the functions contained within the building or reflect important historical considerations. Proposals for naming of new facilities, changing the name of an existing facility, or naming a previously undesignated area shall be considered only upon submission of a written request and justification for the proposed name to the President.

In addition to functional or historically derived names, recommendations to name buildings and other facilities for individuals who have made exemplary or meritorious contributions of service to the University, or to recognize significant and substantial private gifts may also be considered upon presentation of written justification. Normally, the naming of buildings and other facilities in honor of campus officials, faculty or staff, or selected or appointed public officials shall normally occur only after the campus employment or public service has concluded.

Significant contributions are defined as those having a lasting positive impact on the programs and activities of students and faculty, and which further the educational, research, and public service purposes of the University. Normally, substantial means a considered and reasonable relationship between the dollar value of the donation or donations and the size and stature of the facility being recommended for naming.

Upon receipt of a recommendation for the naming of a building or other facility, the President may seek such consultation on the proposal as may be considered appropriate. If the President concurs with the request, a recommendation will be forwarded for consideration and action by U. T. System Administration and the Board of Regents of the University of Texas System.

No action, formal or informal, shall be taken to implement a recommendation for the naming of a building or other facilities until final approval is obtained from the Board of Regents. No commitment, direct or implied, shall be made to any party regarding the naming of a building or facility prior to receipt of approval by the Board of Regents of a private development plan which incorporates the naming of facilities as recognition of significant and substantial gifts, or of a singular recommendation for an individual building or other facility.

Chapter 7: Inclement Weather Policy

7.1 Inclement Weather Conditions

Any decision to close The University of Texas at El Paso during severe weather will be made after several factors are considered, including current and forecasted weather conditions, street conditions and any decision made by the major public school districts to cancel classes. Information concerning weather, road conditions and the status of the University campus physical facilities will be gathered by the Vice President for Business Affairs and transmitted to the President.

The President shall make the decision to close the University due to inclement weather. In the absence of the President, the decision to close University offices and suspend classes will be made by the Vice President for Business Affairs.

7.2 Notification

If a decision is made by the President to close the University, the Provost, the Vice President for Student Affairs, the Vice President for Institutional Advancement, the Vice President for Research and Sponsored Projects, University Communications Office, and the University Police will be notified immediately by the Vice President for Business Affairs. The Vice Presidents will assume responsibility for notifying key supervisory personnel in their respective divisions.

The Director of University Communications will notify all local news media. Every effort will be made to notify area television and radio stations no later than 6:00 a.m. if the University is to be closed for all or part of the day.

Inquiries regarding closure of the University during periods of extreme weather should be directed to the University Police department or University Communications.

7.3 Closing of the University

A decision to close the University will result in suspension of all classes and closure of most offices. During such times, students, faculty, and staff, will not be expected to perform their normal work assignments. The following offices, however, will remain open to provide essential services:

- University Police
- Telecommunications
- U.S. Post Office-Union
- Student Housing

Other essential services determined by each Vice President

Employees who are required to work when the University is closed because of inclement weather will, if eligible, earn equivalent compensatory time for the hours they work.

7.4 Absence During Inclement Weather

During periods of severe weather members of the faculty or staff who cannot travel safely are expected to notify their Department Chair or Director by phone unless there has been an official announcement that the University has been closed. When the University is open, all faculty and staff members are expected to make a reasonable effort to meet their assigned responsibilities. Hours of work missed by staff members, while the University is open, must be charged to vacation leave or earned compensatory time, or leave without pay, if no vacation leave or compensatory time is available. (Minor periods of tardiness will be excused. However, lengthy periods should either be made up in the same work week or charged to annual leave, or leave without pay, as appropriate.)

Absences by faculty members will be handled in accordance with current academic policies.

Chapter 8: Electronic Access and Control Policy

8.1 Purpose

Describe Electronic Access Control procedures and responsibilities for University granted electronic access.

8.2 Applicability

Applies to all University departments.

8.3 Policy

8.3.1 Routine access to locked University facilities or areas within University facilities required for the performance of an employee's assigned duties will be provided through the granting of electronic access.

8.3.2 Electronic access to building, offices, and other facilities may only be granted to a University employee upon proper authorization by a Department.

- a.** Electronic access may not be granted to a student unless the student has a University appointment as an Assistant Instructor, Teaching Assistant or Research Assistant, or the University Department or Office requesting the electronic access for a student requests an exception.

8.4 Procedures

8.4.1. The Department will be responsible for initiating requests for electronic access to be granted to their faculty, staff and student employees.

8.4.2. The designated Department administrator must submit a properly completed electronic access request form to the Facilities Services Key Shop and provide the following information.

- a.** Name of the person to whom electronic access is granted and their identification number assigned by the University Miner Gold Card office (only one name per electronic access request form).
- b.** Building for which electronic access is to be granted (one item per line). Specify the days of the week and time frames access is granted. Include a start date and end date for electronic access.
- c.** Room Number(s) for which electronic access is to be granted (one item per line).
- d.** Signature and extension of person to whom electronic access is granted.
- e.** Signature of designated Department administrator authorizing the access.
- f.** Justification for exception to student access policy as indicated in section 8.3.2.a above.

8.4.3. The Department should have an internal Access Control process and/or procedures to track all electronic access granted upon request by the Department.

8.4.4. Persons to whom University electronic access is granted must acknowledge to the department that they will assume full responsibility for the proper use of electronic access they are granted. The electronic access recipient also agrees that they:

- a.** will not lend or otherwise permit their Miner Gold Card to be used by any other person to gain electronic access to spaces;
- b.** will report the loss or theft of their Miner Gold Card within 24 hours as per the Lost Key Procedures;
- c.** will use the electronic access granted to gain access only to the assigned work area(s) to conduct University business; and
- d.** will ensure the door(s) to assigned work area(s) is/are properly locked or otherwise secured when leaving the area(s) or at the conclusion of work.

8.4.5. Once Electronic Access requests are processed, access will be granted within 24 -48 hours after date of receipt. Electronic access requests with erroneous or missing information will not be processed and will be returned to the department for corrections.

Updated: April 23, 2009

Chapter 9: Banners

9.1. Banners

Please refer to the next section.

9.1.1 Banners

9.1.1.1 “Banners” has the same meaning established in Section 2.5.4.1 of Chapter 2, Student Affairs Section of this Handbook.

9.1.1.2 The President of the University shall authorize places where banners may be hung by any academic or administrative unit.

9.1.1.3 Academic and administrative units, faculty, and staff organizations may hang banners established in this section. Individuals may not hang banners.

9.1.1.4 Advance permission is required from the President of the University, and usually, advance reservations are required. Academic and administrative units advertising official University events or programs may be given priority. In locations administered by academic or administrative units other than the Dean of Students, organizations affiliated with the unit administering the location may be given priority.

9.1.1.5 In locations administered by the President of the University, each banner may be hung for one week. The banner may be renewed from week to week if space is available, but usually, other organizations are waiting their turn and renewal is not possible. The President of the University may limit the time each banner may hang. Any such time limit shall be applied without discrimination to all organizations, except that academic and administrative units may be given preference.

9.1.1.6 The unit requesting a banner location must require that the physical work of hanging the banners be performed only by employees of Facility Services or other appropriate University personnel. Actual costs will be charged to the organization or unit making the request.

Updated: August 17, 2009