Acceptable Use Policy

1.0 Introduction

The University of Texas at El Paso's (“UTEP”, also referred to as the “University”) intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to the University's established culture of openness, trust and integrity. The University is committed to protecting its employees, partners and the institution from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/intranet/extranet-related systems, including but not limited to computer, devices using University resources, equipment, software, operating systems, storage media, and network accounts providing electronic mail (e-mail), web browsing, and FTP are the property of UTEP. These systems are to be used for business purposes in serving the interests of the University, and of our clients and customers in the course of normal operations.

Effective security is a team effort involving the participation and support of every UTEP user, employee and affiliate who deals with information or information resources. It is the responsibility of every system user to know these guidelines, and to conduct their activities accordingly.

2.0 Purpose

Under the provisions of the Information Resources Management Act, Information Resources are strategic assets of the State of Texas that must be managed as valuable state resources. Thus this policy is established to achieve the following:

- Ensure compliance with applicable statutes, regulations, and mandates regarding the management of information resources.
- Establish prudent and acceptable practices regarding the use of Information Resources.
- Educate individuals who may use Information Resources with respect to their responsibilities associated with such use.

3.0 Scope

This policy applies to all individuals granted access privileges to any University Information Resource regardless of affiliation. This policy applies to all equipment that is owned or leased by the University.

4.0 General Use and Ownership

While UTEP's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on University systems remains the property of the University. Because of the need to protect UTEP's network, management cannot guarantee the confidentiality of information stored on any network device belonging to the University. Electronic files created, sent, received, or stored on Information Resources owned, leased, administered, or otherwise under the custody and control of the University are not private and

Revised 01/05/2012 Page 1
may be accessed by UTEP Information Security Office (ISO) employees at any time without knowledge of the Information Resources user or owner.

Electronic file content may be accessed by appropriate personnel in accordance with the provisions and safeguards provided in the Texas Administrative Code §202, Information Security Standards.

Users are responsible for exercising good judgment regarding the reasonableness of personal use. If there is any uncertainty, the user should consult their supervisor or manager, Dean of Students or HelpDesk, as appropriate.

The ISO recommends that any information that users consider confidential or vulnerable be encrypted. For guidelines on encrypting e-mail and documents, see the Acceptable Encryption Policy.

For security and network maintenance purposes, authorized individuals within the University may monitor equipment, systems and network traffic at any time, per the Audit Policy.

UTEP reserves the right to audit all networks and systems on a periodic basis to ensure compliance with this policy.

UTEP encourages everyone associated with the University to act in a manner that is fair, mature, respectful of the rights of others, and consistent with the educational purposes of the University.

By their use of the UTEP network, users acknowledge that the Internet contains access to pornographic and other material that may be offensive to others and unsuitable for minors. UTEP ordinarily does not filter, censor, edit, or regulate the flow of data, software, graphic images, or other materials on the Internet to or from any of its account holders. The Internet may from time to time contain hostile programs, viruses, worms, Trojan horses and other files that may affect or destroy the operation of or information on the computer.

The University is not responsible for the content, accuracy or reliability of information accessed from the Internet. Users are encouraged to verify the authenticity and accuracy of materials sent/received via the Internet, and to use good judgment when deciding whether to download or open materials from people they do not know and organizations they did not contact.

The University of Texas at El Paso will not be liable for missing or misdirected e-mail. UTEP is not responsible for the loss of files or materials due to deletion, error or malfunction, and users are advised to maintain backup copies of their materials at all times.

Users agree to comply with this University policy, the University’s Information Resources Usage Policy, Information Security Polices, other University rules governing acceptable use of information technology, and any applicable state and federal regulations. The terms and conditions of these policies, rules, procedures, and agreements are subject to change without prior notice. Notice of such changes, at the University’s discretion, may be given by posting on the Internet, by e-mail, or other means.
Users must report any weaknesses in UTEP network or computer security and any incidents of possible misuse or violation of this agreement to the proper authorities by contacting the HelpDesk or the Information Security Office (ISO).

Users must not attempt to access any data or programs contained on UTEP systems or network for which they do not have authorization or explicit consent by the proper University official.

Users must not grant access to any University resource without the prior approval of the ISO and Data Owner.

Users must not divulge Dial back modem telephone numbers to anyone.

Users must not share their UTEP account(s), passwords, Personal Identification Numbers (PIN), security tokens (i.e. Smartcard, etc.), or similar information or devices used for identification and authorization/authentication purposes.

Users must not make or distribute unauthorized copies of copyrighted software or material.

Users must not purposely engage in activity that may: harass, threaten or abuse others; degrade the performance of Information Resources; deprive an authorized UTEP user access to a University resource; obtain extra resources beyond those allocated or circumvent UTEP computer security measures.

Users must not download, install or run security programs or utilities that reveal or exploit weaknesses in the security of a system/network. For example, users must not run password cracking programs, packet sniffers, or port scanners or any other non-approved programs on University Information Resources. Only the ISO may grant exemptions to this rule.

University Information Resources must not be used for personal benefit.

Access to the Internet from a UTEP-owned, off-campus or home-based computer must adhere to all policies that apply to use from within The University of Texas at El Paso facilities. Employees must not allow family members or other non-employees to access UTEP computer systems.

Users using University resources or connecting to University resources with a personal or non-UTEP owned system will be held responsible to adhere to all University policies and procedures.

Users must not engage in acts against the aims and purposes of the University as specified in its governing documents or in rules, regulations or procedures adopted from time to time.

Users agree to follow normal standards of ethics and polite conduct in their use of shared computing/networking resources.

Users should follow the same standards of conduct when interacting on the network as when interacting in person.
Laws and rules against fraud, harassment, obscenity, and the like apply to electronic communications just as they apply to other media. Inappropriate distribution, downloading, or sharing of copyrighted materials such as, but not limited to, computer software, movies, and music is a violation of federal law and University rules.

Violation of these laws or rules, or allowing access to others who violate them, will result in terminated of network access and users may be subject to civil or criminal penalties or disciplinary action by the University as applicable.

Users agree that they are solely responsible for making sure that any information they access, share, distribute, upload, or transmit (including information obtained through any hyperlink) complies with applicable law.

The network connection supplied by the University for Miner Village or Miner Heights residents is for individual use and may not be shared among multiple users. Individuals are responsible for all charges and for all destructive or illegal activity done by anyone to whom they allow access.

Student violators of University rules and policies may be referred to the Dean of Students for disciplinary action. The Dean of Students will be notified of violations of University rules and policies, and will take appropriate disciplinary action, up to and including expulsion.

The University, using generally accepted standards of best network administration practices and procedures, has the right to determine what activities disrupt the network. The University further reserves the right to terminate the connection of any host using an unusually high portion of bandwidth if that program unreasonably inhibits the fair use of network resources by other University users or members of the UTEP community.

Users agree that delay of the University to immediately respond to a violation does not prevent the University from taking corrective action at a later time.

**Users agree NOT to:**

- Use network access for solicitations, commercial purposes, or any business activities for individuals, groups, or organizations.
- Modify or tamper with network services, wiring, and ports in any room without explicit written permission. This includes extending the network beyond the single network outlet (using a wireless hub for example, Remote Access Servers, tunneling NETBIOS, or Proxies).
- Establish servers for anything other than academic purposes or provide other activities that consume a disproportionate share of bandwidth (Examples of servers that would be prohibited include, but not limited to, music, movie, television show, or Game servers, etc.).
- Register an outside domain host name that refers to an IP address within the utep.edu domain.
- Scan for systems on any network using port scanners or network probing software.
- Use defective or malfunctioning equipment on the network. Violation of this agreement will result in the offending port(s) being disabled without prior notification.
- Use any connection to engage in any unlawful purpose or share and/or transmit material that violates applicable local, state or federal laws or University rules.
5.0 Unacceptable Use

The following activities are, in general, prohibited:

Under no circumstances is an employee, user or anyone else authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing UTEP-owned/managed information resources.

Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the University.

Unauthorized downloading, copying, sharing, or distribution of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, copyrighted movies, copyrighted television shows, and the installation of any copyrighted software for which the University or the user does not have an active license.

Exporting a device, software, technical information, encryption software or technologies, in violation of international or federal export control laws. Appropriate management should be consulted prior to export of any material that is in question.

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

Revealing an account password to others or allowing the use of an authorized University account by others. This includes family and other household members when work is being performed at off-campus.

Using a UTEP computer to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

Making fraudulent offers of products, items, or services originating from any UTEP Information Resources.

Making statements about warranty, expressed or implied, unless it is a part of normal job duties.

Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the user is not an intended recipient or logging into a system, server or account that the employee or user is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, ping floods, packet spoofing, denial of service attacks, spamming, and forged routing information for malicious purposes.

Executing any form of network monitoring that will intercept data not intended for the user's host, unless this activity is a part of the employee's normal job duty.
Circumventing user authentication or security of any host, network or account.

Interfering with, or denying service to, any user other than the employee's host (for example, denial of service attack).

Using any program/script/command/etc., or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session or the University's Information Resources, via any means, locally or via the Internet.

Providing information about, or lists of, University held information to unauthorized parties outside of the University.

Sending unsolicited e-mail messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (e-mail spam).

Any form of harassment via e-mail, telephone, or paging, whether through language, frequency, or size of messages.

Unauthorized use, or forging, of e-mail header information.

Solicitation of e-mail for any other e-mail address, other than that of the poster's account, with the intent to harass or to collect replies.

Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

Use of unsolicited e-mail originating from within the University's networks or other Internet Service Providers (ISP) on behalf of, or to advertise, any service hosted by the University or connected via the University's network.

Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

Sending broadcast messages through means that are not approved.

6.0 Incidental Use

As a convenience to The University of Texas at El Paso user community, incidental use of Information Resources is permitted. The following restrictions apply:

- Incidental personal use of electronic mail, Internet access, fax machines, printers, copiers, etc., is restricted to The University of Texas at El Paso approved users; it does not extend to family members or acquaintances.
- Incidental use must not result in direct cost to The University of Texas at El Paso.
- Incidental use must not interfere with the normal performance of an employee's work duties.
- No files or documents may be sent or received that may cause legal action against, or embarrassment to, The University of Texas at El Paso.
- Storage of personal e-mail messages, voice messages, files and documents within The University of Texas at El Paso's computer systems must be minimal.
• All messages, files and documents located on The University of Texas at El Paso Information Resources are owned by The University of Texas at El Paso. They may be subject to open records requests and may be accessed in accordance with this policy.

7.0 E-Mail

The University of Texas at El Paso provides electronic mail (e-mail) accounts to all faculty, staff, students, and non-university personnel who are affiliated with the University and are assisting the University in meeting its mission. Official business of the University will be conducted using University-furnished e-mail addresses, in the format user@utep.edu for employees and other non-university personnel, and user@miners.utep.edu for students. For this reason, all users are strongly urged to obtain an official UTEP e-mail address.

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

• Transmission, display, printing or storage of any material prohibited by law or University policies and regulations.
• Unauthorized transmission, display, printing or storage of legally restricted or confidential material.
• Transmission, display, printing or storage of material that is obscene, libelous, or physically threatening.
• 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.
• Transmission, display, printing, or storage of any material through the fraudulent use of another person’s password. Any use of another person's password for any purpose is prohibited.
• 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. Only upon approval of the President or a Vice President of the University may a general broadcast message (e-mail bulletin) be placed in the e-mail system.
• Sending e-mail that is intimidating or harassing.
• Using e-mail for conducting personal business.
• Using e-mail for purposes of political lobbying or campaigning.
• Violating copyright laws by inappropriately copying, sharing, and distributing protected works.
• Posing as anyone other than oneself when sending e-mail, except when authorized to send messages for another when serving in an administrative support role.
The following activities are prohibited because they impede the functioning of network communications and the efficient operations of electronic mail systems:

- Sending or forwarding chain letters.
- Sending unsolicited messages to large groups except as required to conduct agency business.
- Sending excessively large messages or attachments.
- Sending or forwarding e-mail that is likely to contain computer viruses or malware.

All confidential UTEP material transmitted over external network must be encrypted.

All user activity on UTEP Information Resources assets is subject to logging and review without prior notification.

The content, maintenance, and 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.

Electronic mail users must not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of the University or any unit of the University unless appropriately authorized (explicitly or implicitly) to do so. Where appropriate, an explicit disclaimer will be included unless it is clear from the context that the author is not representing the UTEP. An example of a simple disclaimer is: "the opinions expressed are my own, and not necessarily those of my employer."

Individuals must not store, send, forward or receive confidential or sensitive University information through e-mail unless the information is appropriately encrypted or password-protected. Please note that if using a password, it must not be transmitted along with the password-protected file, and it must meet the minimum password requirements as set forth in UTEP’s Information Security Policies. It is best to call the individual and give them the password over the telephone.

Individuals must not store, send or forward confidential or sensitive University information utilizing non-UTEP e-mail accounts. Examples of non-University e-mail accounts include, but are not limited to, Hotmail, Yahoo mail, AOL mail, Google mail, SBCGlobal mail, Roadrunner mail, etc. or e-mail provided by other Internet Service Providers (ISP).

Individuals must not send, forward, receive or store confidential or sensitive University information utilizing non-University accredited mobile devices. Examples of mobile devices include, but are not limited to, Personal Data Assistants (PDA), iPads, tablets, two-way pagers, cellular telephones, etc.

Individuals must exercise utmost caution when sending any e-mail from inside the University to any outside network. Unless approved by the ISO, UTEP e-mail will not be automatically forwarded to an external destination. Confidential information, as defined in the UTEP Information Security Policies (see “Passwords”), should not be forwarded via any means, unless that e-mail is critical to University business and is encrypted/password-protected in accordance with the Acceptable Encryption Policy and/or by contacting security@utep.edu.
8.0 Disciplinary Actions

Violation of this policy may result in disciplinary action that may include termination of employees or suspension or expulsion in the case of a student. Additionally, users are subject to loss of University Information Resources access privileges and may face civil and criminal prosecution.

All users are responsible for managing their use of Information Resources and are accountable for their actions relating to Information Resources security. Users are also equally responsible for reporting any suspected or confirmed violations of this policy to the appropriate management.

The use of Information Resources must be for officially authorized business purposes only. There is no guarantee of personal privacy or access to tools such as, but not limited to, e-mail, web browsing, and other electronic discussion tools. The use of these electronic communication tools may be monitored to fulfill complaint or investigative requirements.

Departments responsible for the custody and operation of systems shall be responsible for proper utilization of Information Resources under their control, as well as the establishment of effective use methods, and providing any required reports to management. Departments must provide adequate access controls in order to monitor systems to protect data and programs from misuse in accordance with the needs defined by owner departments. Access must be properly documented, authorized and controlled.

The user must keep any data used in an Information Resources system confidential and secure. The fact that the data may be stored electronically does not change the requirement to keep the information confidential and secure. Rather, the type of information or the information itself is the basis for determining whether the data must be kept confidential and secure. Furthermore, if this data is stored in a paper or electronic format, or if the data is copied, printed, or electronically transmitted the data must still be protected as confidential and secured appropriately.

All computer software programs, applications, source code, object code, documentation and data shall be guarded and protected as if it were state property.

All commercial software used on computer systems must be supported by a software license agreement that specifically describes the usage rights and restrictions of the product. Personnel must abide by all license agreements and must not illegally copy licensed software. The University reserves the right to remove any unlicensed software from any system at any time without prior notification.

9.0 Security and Proprietary Information

The user interface for information contained on Internet/intranet/extranet-related systems should be classified as either confidential or not confidential, as defined by the Public Information Handbook, of the Office of the Attorney General for the State of Texas. The following standard exists in addition to other University policies and federal and state regulations governing the protection of the University’s data: The University of Texas at El Paso Information Security Office Data Classification Standards. Employees should take all necessary steps to prevent unauthorized access to confidential information. Keep passwords
secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System-level passwords should be changed every 90 days; user-level passwords should be changed at least once annually.

All portable computing devices, laptops, workstations, iPads, tablets, etc. should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off when the host is expected to be left unattended. Encrypt information in compliance with the Acceptable Encryption Use Policy. Because information contained on portable computing devices are especially vulnerable, the Information Security Office encourages the use of multi-passwords if available, encryption of the hard disk contents, and physical cables or locks attached to the computer or laptop if applicable. All systems connecting to University Information Resources (e.g., network, wireless, physical, VPN, etc.) must comply with UTEP’s Information Security Policies.

Postings by a UTEP employee to newsgroups, blogs, etc. should contain a disclaimer stating that the opinions expressed are strictly his/her own and not necessarily those of The University of Texas at El Paso, unless posting is in the course of business duties. All hosts used by a user, employee or student that are connected to University Information Resources, whether owned by the user, employee, or the University, shall be required to continually execute approved virus-scanning software with a current virus database unless overridden by departmental policy. Users must use extreme caution when opening e-mail attachments received from unknown senders as they may contain viruses, e-mail bombs, or Trojan horse code.

10.0 References

The University of Texas at El Paso Information Security Policies
The University of Texas at El Paso Handbook of Operating Procedures, Section VIII: Facilities, Safety, Information and Technology
The University of Texas at El Paso ISO Data Classification Standards
Texas Administrative Code (TAC) §202
UTS165-The University of Texas System Information Resources Use and Security Policy
UT System Regents’ Rules and Regulations
The State of Texas Open Records Act
The State of Texas Penal Code, Chapters 33 and 33A
The Office of the Attorney General for the State of Texas, Public Information 2012 Handbook
Texas Government Code, Section 441
DIR Practices for Protecting Information Resources Assets
DIR Standards Review and Recommendations Publications Revision History
Digital Millennium Copyright Act of 1998
Copyright Act of 1976
Foreign Corrupt Practices Act of 1977
Federal Trade Commission 16 CFR Part 681 (Red Flag)
Computer Fraud and Abuse Act of 1986
Federal Educational Rights and Privacy Act (FERPA)
The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
IRM Act, 2054.075(b)
11.0 User Acknowledgment

By connecting to the University’s resources, the User acknowledges that they have read The University of Texas at El Paso Acceptable Use Policy, and understand that by accessing and/or using UTEP Information Resources the user hereby acknowledges that they must comply with the Policy. User further understands that failure to comply with the Policy and all other applicable Policies, Rules and Regulations, may result in cancellation of the user’s privilege of use, appropriate disciplinary action, and action by law enforcement authorities.

Signature: _______________________________
Print Name: ______________________________
Date: ________________________________