The University of Texas at El Paso
Information Security Policies

Table of Contents

Introduction

The usage of Information Resources is evolving and expanding at an unparalleled rate. As this usage grows, so does the possibility of loss or misuse of information. The University of Texas at El Paso (referred to as “UTEP” or “the University”) recognizes that Information Resources are important state assets that must be safeguarded at all times. All of us, as authorized UTEP Information Resource users, have a responsibility to insure that we protect information entrusted to us. These rules and regulations governing Information Resources for UTEP are intended to supplement existing policies published by the Texas Department of Information Resources (DIR), and The University of Texas System (UTS), as well as reinforce the Texas Computer Crimes Law and other laws governing the use or misuse of state property.

Today, users have computing skills that were previously isolated in central IT groups. Robust software, that at one time was only available on mainframe computers, is now available at the desktop. Hardware is more powerful, faster, and cheaper. In our "connected" world, we continuously increase our dependencies on Internet, intranet, and extranets for conducting business functions. Many of our systems are relying on electronic connections with our vendors and our customers. For all of these reasons, information security today is no longer an obscure function of the automation center. Information risk management is considered to be an integrated part of conducting and continuing state business. The pace of change in information technology requires us to continually evaluate and modify our security programs to meet the increasing challenges in protecting our Information Resources. Information is more than a resource; it has the same value characteristics as other state assets. Information technology has given us many new threat potentials for exploitation of our valuable information.

Revision History
First Draft: December 24, 2001
Revised: March 4, 2002
Revised: September 11, 2002
Revised: September 17, 2002
Revised: December 13, 2011

Purpose

These policies are established to:

- Educate employees, students, and others who may use Information Resources about the responsibilities associated with such use.
- Ensure that the University complies with state laws and regulations regarding the use of and security of Information Resources.
- Create prudent and reasonable practices for the use and protection of Information Resources.

By following the policies and procedures specified in this manual, users will comply with all current federal, state and local laws regarding the use and protection of information resources.

While these policies identify many roles and responsibilities in safeguarding information resources, they cannot possibly cover every situation or future development and, in this regard, they are considered to be a "living document" which can be modified or changed as needs require. You are encouraged to submit your suggestions for improvement to: security@utep.edu.

These policies meet the requirements of the Title 1 Texas Administrative Code 202.2 (1 TAC 202.2) and The University of Texas System 165 (UTS165).

These policies are to be distributed to major users as directed by the Chief Information Officer (CIO). They will be posted in computer labs and other locations frequented by faculty, staff and students. They will be made available through the University official website for employees, non-employees, and students. They will be reviewed on a periodic basis for corrections and to insure compliance with current rules and regulations.

Revision History
First Draft: December 24, 2001
Revised: March 4, 2002
Revised: September 11, 2002
Revised: September 17, 2002
Revised: April 17, 2007
Revised: December 13, 2011
Revised: September 30, 2014 – review policies on a periodic basis

Scope

It is the policy of the University to protect all data and information technology resources in accordance with the Texas Department of Information Resources (DIR) Practices for Protecting Information Resources Assets, and Standards, and Guidelines published in the Texas Administrative Code, 1 TAC 202.25(7), and The University of Texas System 165 (UTS165). Under the provisions of the Information Resources Management Act, Section 2054.001 et seq., Government Code ("Act"), University Information Resources are strategic assets of the State of Texas that must be managed as valuable state resources.

These policies apply to Information Resources, which include all computer and telecommunication hardware and software, networks owned, leased, or operated by the University, and the data or information stored therein. They apply to those same resources owned by others, such as political subdivisions of the state or agencies of the state or federal government, in those cases where there is a statutory, contractual, or fiduciary duty to protect the resources while in University custody. If the owner has a more restrictive policy than these policies, then the owner's policy will control.

Revision History
First Draft: December 24, 2001
Revised: March 4, 2002
Revised: September 11, 2002
Revised: September 19, 2002
Revised: April 17, 2007
Revised: May 20, 2011

Roles and Responsibilities

General:

Department heads are responsible for security of Information Resources within their departments. By assuring that personnel comply with these policies, department heads will provide the control necessary to protect the integrity of the Information Resources.

Department heads will identify positions under their supervision that require special trust. Applicants for and incumbents in those positions must be screened, trained, and managed in ways that will ensure an adequate level of security for Information Resources to which they have access.

Chief Administrative Officer:

The Chief Administrative Officer (CAO) is responsible for establishing and maintaining security and risk management programs for Information Resources. Responsibilities include:

- Enforcing state-level security and risk management policies.
- Establishing and maintaining a risk management program.
- Establishing and maintaining policies and procedures that provide for the security of Information Resources.
- Assigning ownership for Information Resources.
- Preparing and maintaining Business Continuity Plan (BCP) for Disaster Recovery (DR).
- Ensuring compliance with Texas Department of Information Resources (DIR) planning requirements by including security and risk management policies and practices in the institution's strategic plan.
- Ensuring compliance with state Information Resources audit requirements.
- Ensuring participation by all levels of management and administrative and technical staff during planning, development, and implementation of policies and procedures.

Information Resources Manager (IRM):

The Information Resources Manager (IRM) is appointed by the President.

The IRM retains ultimate responsibility for enforcement of Business Continuity Plan for Disaster Recovery, all security and risk management policies but may delegate the procedural responsibilities to an individual of their choice.

Chief Information Security Officer (CISO):

The individual responsible for this function shall report to the IRM and is responsible for directing policies and procedures designed to protect Information Resources. This function:

- Monitors University Information Resources
- Identifies vulnerabilities.
- Identifies critical and confidential Information Resources.

- Develops/Maintains a Risk Management Program.
- Develops/Maintains an adequate Security Program.

Owners of Information Resources:

Information Resources are to be assigned "Owners". The Owner is the designated person responsible for carrying out the program that uses the resources. That person is referred to herein as a "Program Manager". At a minimum, the Owner, or Program Manager, is responsible for and authorized to:

- Assess and classify information.
- Identify risks to Information Resources through risk analysis.
- Work with technical management to specify cost effective security controls and convey security control requirements to users and custodians.
- Approve access and formally assign custody of the Information Resources.
- Ensure compliance with applicable controls.
- Plan for business continuity, contingencies and disaster recovery for the Information Resources.

Custodians of Information Resources:

The "Custodian" is the individual responsible for physical possession of Information Resources (e.g., data owner, data steward, data processing director, network services director, etc.) and for providing the technical facilities, data processing, and other support services to Owners and Users of Information Resources.

As a general rule, the Custodian of Information Resources is assigned the responsibility to:

- Implement the security controls specified by the Owner.
- Provide physical and procedural safeguards for Information Resources within the facility.
- Assist Owners in evaluating the cost-effectiveness of controls.
- Administer access to the Information Resources and make provisions for timely detection, reporting, and analysis of actual and attempted unauthorized access to information resources.

Technical Management:

Technical managers who have been assigned custodial responsibility for the Information Resources utilized in carrying out their technical activities (services) are also responsible for ensuring the security of those resources. In general, technical managers are responsible for:

- Ensuring that adequate technical support is provided to define and select cost-effective security controls.
- Ensuring the implementation of security controls as defined by the owners of the Information Resource and those required to notify the owner of actual and attempted security violations.

- Developing and maintaining business continuity, contingency and disaster recovery plans.
- Developing and following procedures for reporting on monitored controls.

Security Administrators/System Administrators:

Security Administrators/System Administrators are responsible for:

- Providing assistance to the individual(s) responsible for the information security function.
- Assisting with acquisition and maintenance of security hardware/software.
- Assisting with identification of vulnerabilities.
- Developing/maintaining access control rules.
- Maintaining user lists, password control, encryption keys, etc.

Internal Auditor:

The internal audit function of System Administration or the Component is responsible for the periodic, risk-based review of Information Resources security policies and procedures for:

- Compliance with security policies, standards, and guidelines.
- Evaluation of the effectiveness of security controls.
- Examination of planned security controls.
- Participation in the risk analysis process.

Revision History
First Draft: December 24, 2001
Revised: March 4, 2002
Revised: September 11, 2002
Revised: September 17, 2002
Revised: September 10, 2003
Revised: May 26, 2011

General

In support of its mission of teaching, research, and public service, The University of Texas at El Paso provides access to Information Resources for employees and students to the extent permitted by the financial resources of the University and as reflected within established institutional priorities.

The access granted to authorized individuals (e.g., employees, students, vendors, contractors, etc.) to the University's Information Resources is a privilege, not a right. The University may limit, restrict, deny or extend access to its Information 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 Resources. Information Resources (e.g., equipment, systems, network traffic, etc.) usage may be subject to security testing and monitoring by Information Security Office authorized individual(s) within the University at any time without the knowledge of the Information Resources user or owner.

Authorized users of University Information Resources are:

- University students who are limited to the use of those Information Resources specifically assigned to serve educational purposes.
- University employees who are provided access to those Information Resources required for the performance of their duties in the conduct of official business. Access to any particular administrative data file/system must be based on an employee's "need to know" as established by their official duties and reflected in the advance provision of specific authorization codes, passwords or other access-enabling means to the employee. The principle of least privilege will be applied. (See also Account Management, User Roles and Separation of Duties Policy)
- Non University-affiliated individuals or entities after written agreement for purposes related to the University's missions.

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

All users, by accessing any Information Resources of the University, agree to the following:

- Unauthorized use is strictly prohibited.

- Usage by authorized/unauthorized individual(s) may be subject to security testing and monitoring without the prior knowledge of the Information Resources user or owner.
- Abuse is subject to criminal prosecution.
- Not to disclose an assigned password to another person.

Because all files created or maintained using the University's Information Resources are properties 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.

Violators of these policies may be subject to prosecution under applicable criminal or civil laws 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 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, the appropriate authority will pursue further administrative action. This procedure may result in:

- The temporary or permanent loss of access to Information Resources for the offending individual.
- Any other penalty deemed appropriate by a University disciplinary authority upon a finding or admission of guilt following normally afforded due process procedures.
- Criminal prosecution.
- Any combination of the above.

Policy violations by students are handled by The Dean of Students in accordance with The 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 systems, or to make intentionally harmful use of such systems or data files. The seriousness of such a crime ranges from a Class B misdemeanor to a third-degree felony. The University will prosecute all cases of unauthorized access to, or intentional damage or misuse of, University Information Resources.

Revision History
First Draft: December 24, 2001
Revised: March 5, 2002
Revised: September 11, 2002

Revised: September 17, 2002
Revised: April 7, 2003
Revised: December 13, 2011
Revised: September 30, 2014

Acceptable Encryption

1.0 Purpose

The purpose of this policy is to provide guidance that limits the use of encryption to those algorithms that have received substantial public review and have been proven to work effectively. Additionally, this policy provides direction to ensure that Federal regulations are followed, and legal authority is granted for the dissemination and use of encryption technologies outside of the United States.

2.0 Scope

This policy applies to all University of Texas at El Paso employees and affiliates.

3.0 Policy

Proven, standard algorithms such as AES-256, Blowfish, RSA, SHA-256, RC5 and TDEA should be used as the basis for encryption technologies. These algorithms represent the actual cipher used for an approved application. Symmetric cryptosystem key lengths must be at least 256 bits. Asymmetric crypto-system keys must be of a length that yields equivalent strength. The University of Texas at El Paso's key length requirements will be reviewed annually and upgraded as technology allows.

The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed by qualified experts outside of the vendor in question and approved by the Information Security Office (ISO). Be aware that the export of encryption technologies is restricted by the U.S. Government. Residents of countries other than the United States should make themselves aware of the encryption technology laws of the country in which they reside.

4.0 Export Control Regulations

Under export control regulations, any individual transporting a laptop with encrypted data must seek an export license. Because most encrypted data or technology is by nature confidential information or contains controlled technology, licensing may be required under Export Administration Regulations (EAR) or International Traffic in Arms Regulations 2009 (ITAR) in order to be able to “export or re-import” an encrypted system outside or back into the United States. Therefore data considered an Information Resource or otherwise confidential in nature by The University of Texas at El Paso shall not be transported out of the country.

It is recommended that if you are taking a laptop or any other data storage device(s) out of the country, it should only contain public domain information and should not be encrypted. Please contact the Information Security Office if you have any questions.

5.0 Enforcement

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

Revision History
First Draft: December 24, 2001
Revised: January 10, 2002
Revised: March 27, 2002
Revised: September 17, 2002
Revised: December 8, 2006 – Removal of DES and addition of AES. Change of 56 bits to 128 bits.
Revised: May 24, 2011 – Change from 128 bits to 254 bits to match industry standards. Add EAR and ITAR regulations for export, re-import requirements of encrypted system /device outside, or back into the United States.
Revised: December 9, 2016 – Removal of SHA, IDEA and AES to reflect SHA-256, TDEA, AES-256

Acceptable Use

All individuals granted access to or use of System Information Resources must be aware of and agree to abide by **The University of Texas at El Paso Acceptable Use of Information Resources and Security Policy Agreement located here:**

http://admin.utep.edu/Portals/1805/PDF/Acceptable%20Use%20of%20Information%20Resources-Jun2014.pdf

Revision History

First Draft: December 24, 2001
Revised: January 10, 2002
Revised: March 14, 2002
Revised: April 2, 2002
Revised: April 24, 2002
Revised: September 11, 2002
Revised: September 17, 2002
Revised: November 18, 2003
Revised: April 17, 2007
Revised: January 23, 2012
Revised: June 18, 2014

Account Management

1.0 Introduction

Computer accounts are the means used to grant access to UTEP's Information Resources. These accounts provide a means of providing accountability, a key to any computer security program, for Information Resources usage. This means that creating, controlling, and monitoring all computer accounts is extremely important to an overall security program.

2.0 Purpose

The purpose of the UTEP Account Management Security Policy is to establish the rules for the creation, monitoring, control and removal of user accounts.

3.0 Scope

The UTEP Account Management Security Policy applies equally to all individuals with authorized access to any UTEP Information Resources.

4.0 Policy

All accounts created must have an associated request and approval that is appropriate for the UTEP system or service.

All accounts must be uniquely identifiable using the assigned user name.

All default passwords for accounts must be constructed in accordance with the UTEP Password Policy.

All accounts must have a password expiration that complies with the UTEP Password Policy.

Accounts of individuals on extended leave (more than 30 days) will be disabled.

All new user accounts that have not been accessed within 30 days of creation will be disabled.

Data Owners, System Owners, System Administrators and/or other authorized personnel:

- are responsible for removing the accounts of individuals that change roles within the University or are separated from their relationship with UTEP
- must have a documented process to modify a user account to accommodate situations such as name changes, accounting changes and permission changes
- must have a documented process for periodically reviewing existing accounts for validity
- are subject to independent audit review
- must provide a list of accounts for the systems they administer when requested by the Information Security Office

- must cooperate with Information Security Office personnel investigating security incidents

Separation of Duties

Information Systems access should be designed to maintain separation of duties to reduce the risk of a malicious individual performing conflicting activities (i.e. requesting system access while also approving one's own system access). Compensating controls such as log monitoring and system-enforced thresholds may also be implemented when conflicting duties cannot be separated. The principles of least privilege will be applied to all users when access is required to perform their business function.

Users

All Users must comply with this UT System Policy for Use and Security of Information Resources (UTS165). Users who fail to comply are subject to disciplinary action.

7.0 Disciplinary Actions

Violation of this policy may result in disciplinary action which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of UTEP Information Resources access privileges, civil, and criminal prosecution.

Revision History
First Draft: April 2, 2002
Revised: September 17, 2002
Revised: May 24, 2011
Revised: September 30, 2014

Administrative/Special Access

1.0 Introduction

Technical support staff, security administrators, system administrators and others may have special access account privilege requirements compared to typical or everyday users. The fact that these administrative and special access accounts have a higher level of access means that granting, controlling and monitoring these accounts is extremely important to an overall security program.

2.0 Purpose

The purpose of the UTEP Administrative/Special Access Practice Standard is to establish the rules for the creation, use, monitoring, control and removal of accounts with special access privilege.

3.0 Scope

The UTEP Administrative/Special Access Practice Standard applies equally to all individuals that have, or may require, special access privilege to any UTEP Information Resources.

4.0 Policy

University departments must submit a list of administrative contacts (e.g., data owners, system owners, system administrators, etc.) to the Information Security Office (ISO) for systems that are connected to the UTEP network.

All users must sign the Acceptable Use Policy and Nondisclosure Agreement before access is given to an account.

All users of Administrative/Special access accounts must have account management instructions, documentation, training, and authorization.

Each individual that uses Administrative/Special access accounts must refrain from abuse of privilege and must only do investigations under the direction and prior approval of the CISO or executive management.

Each individual that uses Administrative/Special access accounts must use the account privilege most appropriate with work being performed (i.e., user account vs. administrator account). Individuals are encouraged to use their regular account for day-to-day operations and use the administrative/special access account only when necessary.

Each account used for administrative/special access must meet the requirements of the Password Policy.

The password for a shared administrator/special access account must change when an individual with the password leaves the department or the University, or upon a change in the vendor personnel assigned to the UTEP contract.

In the case where a system has only one administrator there must be a password escrow procedure in place so that someone other than the administrator can gain access to the administrator account in an emergency situation.

When Special Access accounts are needed for Internal or External Audit, software development, software installation, or other defined need, they:

- must be authorized
- must be created with a specific expiration date
- must be removed when work is complete

5.0 Disciplinary Actions

Violation of this policy may result in disciplinary action which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of UTEP Information Resources access privileges, civil, and criminal prosecution.

Revision History
First Draft: April 2, 2002
Revised: September 17, 2002
Revised: May 25, 2011

Analog/ISDN Line Security

1.0 Purpose

This document explains The University of Texas at El Paso (UTEP) analog and ISDN line acceptable use and approval policies and procedures. This policy covers two distinct uses of analog/ISDN lines: lines that are to be connected for the sole purpose of fax sending and receiving, and lines that are to be connected to computers.

2.0 Scope

This policy covers only those lines that are to be connected to a point inside UTEP building and testing sites. It does not pertain to ISDN/phone lines that are connected into employee homes, PBX desktop phones, and those lines used by Telecom for emergency and non-University information purposes.

3.0 Policy

3.1 Scenarios & Business Impact

There are two important scenarios that involve analog line misuse, which we attempt to guard against through this policy. The first is an outside attacker who calls a set of analog line numbers hoping to connect to a computer that has a modem attached to it. If the modem responds (and most computers today are configured out-of-the-box to auto-answer) from inside the University's premises, then there is the possibility of breaching the University's internal network through that unmonitored computer. At the very least, information resident on that computer may be subject to compromise. This potentially could results in the exposure of University confidential information.

The second scenario is the threat from someone being able to use a modem-equipped laptop or desktop system with physical access to a University facility. In this case, the intruder would be able to connect to the trusted network of the University through the system's Ethernet connection. They could then call out to an unmonitored site using the modem, with the ability to siphon University confidential information to an unknown location. This could also potentially result in the substantial exposure of confidential information.

Specific procedures for addressing the security risks inherent in each of these scenarios follow.

3.2 Facsimile Machines

As a rule, the following applies to requests for fax and analog lines:

- Fax lines are to be approved for departmental use only.
- No fax lines will be installed for personal use.
- No analog lines will be placed in a personal cubicle.
- The fax machine must be placed in a centralized administrative area designated for departmental use, and away from other computer equipment.

- A computer which is capable of making a fax connection is not to be allowed to use an analog line for this purpose.
- Waivers for the above policy on analog-as-fax lines will be reviewed on a case-by-case basis by the ISO after a review is conducted regarding the business need with respect to the level of sensitivity and security posture of the request. A Service Desk Request may be placed and must as a minimum contain the above requested information.
- Use of an analog/ISDN fax line is conditional upon the requester's full compliance with the requirements listed below. These requirements are the responsibility of the authorized user to enforce at all times:
    - The fax line is used solely as specified in the request.
    - Only persons authorized to use the line have access to it.
    - When not in use, the line is to be physically disconnected from the computer.
    - When in use, the computer is to be physically disconnected from UTEP's internal network.
    - The line will be used solely for University business, and not for personal reasons.
    - All downloaded material, prior to being introduced into University systems and networks, must have been scanned by a University-authorized anti-virus utility/scanner which has been maintained current through regular updates.

3.3 Computer-to-Analog Line Connections

The general policy is that requests for computers or other intelligent devices to be connected with analog or ISDN lines from within the University will not be approved for security reasons. Analog and ISDN lines represent a significant security threat to University Information Resources, and active penetrations have been launched against such lines by hackers. Waivers to the policy above will be granted on a case-by-case basis.

Replacement lines, such as those requested because of a move, fall under the category of "new" lines. They will also be considered on a case by case basis.

3.4 Requesting an Analog/ISDN Line

Once approved by a departmental manager, the individual requesting an analog/ISDN line must include the following information:

- A clearly detailed business case as to why other secure connections available at the University cannot be used,
- The business purpose for which the analog line is to be used,
- The software and hardware to be connected to the line and used across the line, and to what external connections the requester is seeking access.
- The business case must answer, at a minimum, the following questions:

    - What business needs are to be conducted over the line?
    - Why is a University-equipped desktop computer with Internet capability unable to accomplish the same tasks as the proposed analog line?

- Why is the University's current dial-out access pool unable to accomplish the same tasks as an analog line?
- In addition, the requester must be prepared to answer the following supplemental questions related to the security profile of the request:
  - Will the machine(s) that is using the analog line be physically disconnected from the University's internal network? Where will the analog line be placed? Specify if other than an office or reception area, in a cubicle or lab?
  - How many lines are being requested, and how many people will use the line?
  - How often will the line be used? Once a week, 2 hours per day...?
  - What is the earliest date the line can be terminated from service? The line must be terminated as soon as it is no longer in use.
  - What other means will be used to secure the line from unauthorized use?
  - Is this a replacement line from an old location? What was the purpose of the original line?
  - What types of protocols will be run over the line?
  - Will a University-authorized anti-virus utility/scanner be installed on the machine(s) using the analog lines?

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Revision History
First Draft: March 27, 2002
Revised: September 17, 2002
Revised: April 27, 2005
Revised: May 25, 2011

Audit

1.0 Purpose

To provide the authority for members of the Information Security Office to conduct security audits on any system at The University of Texas at El Paso.

Audits may be conducted to:

- Ensure confidentiality, integrity, and availability of information and resources
- Investigate possible security incidents and ensure conformance with University policies
- Monitor user and/or system activity where appropriate.

2.0 Scope

This policy covers all computer and communication devices owned, leased, or operated by The University of Texas at El Paso. This policy also covers any computer and/or communications device that is present on The University of Texas at El Paso premises, but which may not be owned or operated by The University of Texas at El Paso.

3.0 Policy

When requested, and for the purpose of performing an audit, any access needed will be provided to members of the ISO team.

This access may include:

- User level and/or system level access to any computing or communications device
- Access to information (electronic, hardcopy, etc.) that may be produced, transmitted or stored on University-owned or leased equipment, or premises
- Access to work areas (labs, offices, cubicles, telecommunications closets, storage areas, etc.)
- Access to interactively monitor and log traffic on the University's networks.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Revision History
First Draft: March 28, 2002
Revised: September 11, 2002
Revised: September 17, 2002
Revised; May 26, 2011

Change Management

1.0 Introduction

The Information Resources infrastructure at UTEP is expanding and continuously becoming more complex. There are more people dependent upon the network, more client machines, upgraded and expanded administrative systems, more web applications, and more application programs. As the interdependency between Information Resources infrastructure grows, the need for a strong change management process is essential. From time to time each Information Resource element requires an outage for planned upgrades, maintenance or fine-tuning. Additionally, unplanned outages may occur that may result in upgrades, maintenance or fine-tuning.

Managing these changes is a critical part of providing a robust and valuable Information Resources infrastructure

2.0 Purpose

The purpose of the Change Management Policy is to manage and document changes in a rational and predictable manner so that staff and clients can plan accordingly. Changes require serious forethought, careful monitoring, and follow-up evaluation to reduce negative impact to the user community and to increase the value of Information Resources.

3.0 Scope

The UTEP Change Management Policy applies to all individuals that install, operate, administer, or maintain Information Resources.

4.0 Policy

Every change to a UTEP Information Resources resource such as, but not limited to,: operating systems, computing hardware, networks, and applications is subject to the Change Management Policy and must follow the Change Management Procedures.

All changes affecting computing environmental facilities (e.g., air-conditioning, water, heat, plumbing, electricity, and alarms) need to be reported to or coordinated with the leader of the change management process.

A Change Management Committee, appointed by Information Security/IRM Leadership, will meet regularly to review change requests and to ensure that change reviews and communications are being satisfactorily performed.

A formal written change request must be submitted for all changes, both scheduled and unscheduled.

All scheduled change requests must be submitted in accordance with change management procedures so that the Change Management Committee has time to review the request, determine and review potential failures, and make the decision to allow or delay the request.

Each scheduled change request must receive formal Change Management Committee approval before proceeding with the change.

The appointed leader of the Change Management Committee may deny a scheduled or unscheduled change for reasons including, but not limited to, inadequate planning, inadequate backup plans, the timing of the change will negatively impact a key business process such as year-end accounting, or if adequate resources cannot be readily available. Adequate resources may be a problem on weekends, holidays, or during special events.

Customer notification must be completed for each scheduled or unscheduled change following the steps contained in the Change Management Procedures.

A Change Review must be completed for each change, whether scheduled or unscheduled, and whether successful or not.

A Change Management Log must be maintained for all changes. The log must contain, as a minimum, the:

- Date of submission and date of change
- Owner and custodian contact information
- System administrator contact information
- Nature of the change
- Indication of success or failure

All UTEP information systems must comply with an Information Resources change management process that meets the standards outlined above.

5.0 Disciplinary Actions

Violation of this policy may result in disciplinary action which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of UTEP Information Resources access privileges, civil, and criminal prosecution.

Revision History
First Draft: April 2, 2002
Revised: September 19, 2002
Revised; May 26, 2011

Database Credentials

1.0 Purpose

This policy states the requirements for securely storing and retrieving database usernames and passwords (i.e., database credentials) for use by a program that will access a database running on one of the University's networks.

Computer programs running on University networks often require the use of one of the many internal database servers. In order to access one of these databases, a program must authenticate to the database by presenting acceptable credentials. The database privileges that the credentials are meant to restrict can be compromised when the credentials are improperly stored.

2.0 Scope

This policy applies to all software that will access a University multi-user production database.

3.0 Policy

3.1 General

In order to maintain the security of the University’s internal databases, access by software programs must be granted only after authentication with credentials. The credentials used for this authentication must not reside in the main, executing body of the program's source code in clear text. Database credentials must not be stored in a location that can be accessed through a web server.

3.2 Specific Requirements

3.21 Storage of Data Base User Names and Passwords

Database user names and passwords may be stored in a file separate from the executing body of the program's code. This file must not be world readable.

Database credentials may reside on the database server. In this case, a hash number identifying the credentials may be stored in the executing body of the program's code.

Database credentials may be stored as part of an authentication server (i.e., an entitlement directory), such as an LDAP server used for user authentication. Database authentication may occur on behalf of a program as part of the user authentication process at the authentication server. In this case, there is no need for programmatic use of database credentials.

Database credentials may not reside in the documents tree of a web server.

Pass-through authentication (i.e., Oracle OPS$ authentication) must not allow access to the

database based solely upon a remote user's authentication on the remote host.

Passwords or pass phrases used to access a database must adhere to the Password Policy.

3.22 Retrieval of Database User Names and Passwords

If stored in a file that is not source code, then database user names and passwords must be read from the file immediately prior to use. Immediately following database authentication, the memory containing the user name and password must be released or cleared.

The scope into which you may store database credentials must be physically separated from the other areas of your code (e.g., the credentials must be in a separate source file). The file that contains the credentials must contain no other code but the credentials (i.e., the user name and password) and any functions, routines, or methods that will be used to access the credentials.

For languages that execute from source code, the credentials' source file must not reside in the same browseable or executable file directory tree in which the executing body of code resides.

4.0 Access to Database User Names and Passwords

Every program or every collection of programs implementing a single business function must have unique database credentials. Sharing of credentials between programs is not allowed.

Database passwords used by programs are system-level passwords as defined by the Password Policy.

Developer groups must have a process in place to ensure that database passwords are controlled and changed in accordance with the Password Policy. This process must include a method for restricting knowledge of database passwords to a need-to-know basis.

5.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Revision History
First Draft: March 29, 2002
Revised: September 17, 2002
Revised: May 26, 2011

Electronic Storage of Confidential Information

1.0 Introduction

The intention of this policy is to communicate requirements for securing, protecting, and ensuring the integrity of UTEP‘s confidential information in any of its forms, whether it be electronic, printed and even memorized information

2.0 Scope

This policy applies to all University of Texas at El Paso employees and affiliates.

3.0 Definitions

Confidential Information - is defined as protected information that is governed by law or contract. [e.g. Health Insurance Portability and Accountability Act (HIPAA), Family Educational Rights and Privacy Act (FERPA), Gramm-Leach-Bliley Act (GLBA/GLB), Sarbanes-Oxley (SOX), Payment Card Industry (PCI), and human subject data]. This includes but is not limited to Social Security Numbers (SSN), UTEP ID numbers, credit card numbers, health and employment records, human subject data, user IDs, passwords, financial information, bank routing numbers, ethnicity, religious affiliation, sexual orientation, political party affiliation, and all FERPA non-directory information about students and former students.

4.0 Policy

This section details steps that must be taken to protect confidential information here at UTEP. Additional policies may apply to the storage of confidential information. Please see UTEP's Information Security Policies, UTEP's Social Security Number Use and Solicitation Policy, and UTS-165 for more information.

4.1 Controlling Access

- Inventory and documentation must be kept of all systems that house confidential information.
- All documents containing confidential information must be password protected.
- Credit card information must be protected in accordance with the Payment Card Industry Digital Security Standards. *Note: Transmission of credit card information unencrypted or through email is strictly prohibited.*
- Confidential documents must not be left in easy to access areas, such as leaving documents or computer equipment on desks that unauthorized people can view or remove. Make sure that you lock and secure all areas when you leave your office.
- Computers left on while unattended shall have a screen saver enabled that is password-protected.
- Computers, laptops, and servers housing confidential information must have the data encrypted.

- Access to confidential information on computers and/or servers must require a combination of a unique login and a secret password that is known only by the user.
- Accounts and passwords must not be shared under any circumstances.
- Storage of confidential information on electronic media must be encrypted or password protected.
- Confidential information may not reside on devices that do not adhere to the system security standards established by the University.
- Confidential information may not be transported outside of the United States without the prior approval of the Information Security Office.
- Accounts that give users access to Information Resources must be used only by the person whom the account is assigned.

4.2 Passwords

- All passwords used to access confidential information on any computer, server, or other electronic device must meet the minimum password complexity standards set by University policy.

4.3 Computer and Server Operation

- Computers and servers used to house confidential information must be kept up-to-date with the latest security patches and antivirus software/virus definition updates.
- The owner of the system should ensure that all of the regular procedures for information security have been followed (change default user names; all accounts are password protected; insure that share access permissions are appropriate and periodically reviewed; remove access as soon as an individual does not require access, transfers to a different department, or is no longer affiliated with the University; etc.).

4.4 Logging and Monitoring

- All computers and servers housing confidential information must log user access to the computer or server (i.e., events, security, and application audit logs must be enabled and must be retained for at least 90-days).
- If confidential information is housed in a program that is capable of tracking user access, this logging must be enabled and must be retained for at least 90-days.

4.5 Miscellaneous

- Transmission of confidential information must be done via an encrypted connection.
- Owners of computers and servers housing confidential information will perform periodic audits to ensure that all outlined security measures are in place.
- Storage of any confidential information on electronic media that does not meet these requirements is prohibited.
- All systems that house confidential information are subject to monitoring and audit by the Information Security Office.

- No confidential information may be displayed in any public way. (For example, in posted lists or mailing labels containing social security numbers or other confidential information).
- Any system that contained confidential information must have the electronic media wiped of all data in accordance with security guidelines before transferring or reallocation of the computer.
- Any system or hard drive that contained confidential information that is transferred to Surplus must be wiped of all data by Surplus in accordance with security guidelines.
- Loss of confidential information through intrusion, theft, or loss of electronic media must be reported immediately to the Information Security Office.

4.6 System Disclaimer/Warning Banner

- All systems that store confidential information must display the following banner.

System Disclaimers
Use of computer and network facilities owned or operated by The University of Texas at El Paso requires prior authorization.
Unauthorized access is prohibited. Usage may be subject to security testing and monitoring, and affords no privacy guarantees or expectations except as otherwise provided by applicable privacy laws. Abuse is subject to criminal prosecution.
Use of these facilities implies agreement to comply with the policies of The University of Texas at El Paso.
OR
This system is for the use of authorized users only. Individuals using this computer system without authority, or in excess of their authority, are subject to having all of the activities on this system monitored and recorded by system personnel.

In the course of monitoring individuals improperly using this system, or in the course of system maintenance, the activities of authorized users may also be monitored. Users (authorized or unauthorized) have no expectation of privacy except as otherwise provided by applicable privacy laws.

Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence of such monitoring to campus officials or law enforcement agencies. By continuing to use this system you indicate your awareness of and consent to these terms and conditions of use.

5.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Revision History

First Draft: May 11, 2006
Approved: July 7, 2006
Revised: March 28, 2007
Revised: September 28, 2007
Revised: May 27, 2011
Revised: December 22, 2015

E-mail Procedures

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. Non-University personnel accounts are sponsored accounts.

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 email
- Define who is eligible for an e-mail account
- Identify the responsibilities of the person assigned an e-mail account
- Identify the responsibilities of the person sponsoring an e-mail account
- Educate individuals on the method for requesting and maintaining e-mail accounts, as well as their responsibilities associated with such use

1.0 Faculty Accounts

Access to faculty is provided based on an active appointment. Visiting faculty can be provided access with approval of the appropriate Dean for the duration of the faculty member's stay at UTEP. Faculty with an active appointment may contact the Technology Support HelpDesk at extension 4357 (HELP) on-campus or (915) 747-5257 off-campus and request an e-mail account. Faculty must contact the Chief Administrative Officer/Administrative Service Officer (CAO/ASO) for their college, department, or division. Upon confirmation of the appointment, an ID and password will be provided.

Visiting faculty should notify the respective CAO/ASO of the sponsoring college so that a sponsored account may be established for the duration of their stay. The ID and password will be provided directly to the visiting faculty member. The sponsor's name will be recorded along with the owner of the account for possible renewal.

Faculty accounts are removed when the member's appointment is terminated. If the account is to remain active after the appointment is terminated, arrangements must be made prior to termination. A letter from the Department Chair must be sent to the HelpDesk requesting an extension. Extensions are granted for 30-day periods with a maximum of 120 days. A new letter must be sent before each expiration period to continue the extension uninterrupted.

2.0 Staff Accounts

Access to staff is provided by the Human Resources Department based on an active appointment. Staff members should contact the Human Resources Department at (915) 747-5202 to request an e-mail ID. Upon confirmation of the appointment, an ID and password will be provided.

Access for contract personnel will be provided upon request from the department head who must contact the HelpDesk with the person's name, UTEP ID, date of birth, and phone

number. The ID and password will be provided directly to the contracted person. Accounts for contract personnel will expire in one month unless the account is requested to be in effect for the duration of the contract. Subsequent requests must be placed to maintain the account in an active status. The sponsor's name will be recorded along with the owner of the account for possible renewal.

Staff accounts are removed when the member's appointment is terminated. If the account is to remain active after the appointment is terminated, arrangements must be made prior to termination. A letter from the Department Chair or Vice President must be sent to the HelpDesk requesting an extension. Extensions are granted for 30-day periods with a maximum of 120 days. A new letter must be sent before each expiration period to continue the extension uninterrupted.

3.0 Student Accounts

All part-time and full-time students actively enrolled at UTEP are eligible for an e-mail account. The e-mail account will be provided on Microsoft's Live@edu system (@miners.utep.edu). This is the official e-mail system for UTEP students. Once a student has an account, they may keep their account active by enrolling in both the spring and fall semesters. The summer semester may be skipped without an interruption of service. The account will remain active for a period of 1 year after last date attended; after which the account will be disabled.

Any student who is also an employee of UTEP will also be provided an e-mail account on UTEP's primary mail system. All business e-mails must be conducted through UTEP's primary e-mail system. It is prohibited to forward e-mail to or conduct any official UTEP related business on any other e-mail system.

4.0 Alumni Accounts

Alumni accounts are retained indefinitely.

5.0 Sponsored Accounts

The University President, Vice Presidents, Deans, Directors, or Chairs may sponsor an e-mail account for non-University personnel who are affiliated with the University and are assisting the University in meeting its mission. Requests must be made to the HelpDesk and the requestor must provide the person's name, UTEP ID, date of birth, estimated period of time the account will be needed, and phone number. Upon approval, an ID and password will be provided. The name of the sponsor will be recorded along with the owner of the account for possible renewal.

Sponsored accounts will expire in December of every year. The sponsor will be notified of an upcoming expiration date or in November asking if they wish to renew the sponsorship. If no response is received, the account will be deactivated as specified above.

6.0 Usage

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 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 the approval of the President or a Vice President of the University may a general broadcast message (e-mail bulletin) be placed on the e-mail system.
- Using email for purposes of political lobbying or campaigning.
- Violating copyright laws by inappropriately distributing protected works.
- Posing as anyone other than oneself when sending email, except when authorized to send messages for another when serving in an administrative support role.
- The use of unauthorized email software.
- Sending or forwarding email that is likely to contain computer viruses.

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. In order to obtain optimum efficiency and service, the system administrator of the e-mail system may delete e-mail messages older than two weeks. E-mail messages requiring retention beyond this time limit should be downloaded to disks or printed for storage by each user.

All user activity on University Information Resource assets may be subject to logging and review, and is the property of The University of Texas at El Paso.

7.0 Expiration of Accounts

When an account is expired, an e-mail notification will be sent to the account owner weekly for two weeks announcing that the account will be expired and providing the web address to this policy for instructions on requesting an extension or reporting a problem. If no action is taken by the owner of the account, i.e., the HelpDesk does not receive a request for an extension, the account will be locked and any files belonging to the account will be retained for two weeks. If the HelpDesk has received no request for extension after the two-week retention period, the account and its files will be permanently removed.

8.0 Problems with Accounts

Problems with an e-mail account should be reported to the HelpDesk at extension 4357 (HELP) from on-campus or (915) 747-5257 from off-campus. Security infractions should be reported to security@utep.edu or to the HelpDesk.

9.0 Complying with Quotas

As a state institution, the University is required to use its resources in an efficient manner. One of the ways it accomplishes this is by the imposition of quotas on e-mail accounts. The user of each e-mail account is given a certain amount of disk space on the e-mail server and must take steps to remain within his/her designated quota or limit. The following steps are intended to help the user delete e-mail that is no longer needed:

- Open Sent Items to display all of the messages you have sent.
- Left mouse click on Edit, choose Select All from the dropdown menu and then click Delete on the Toolbar. This will transfer all of your Sent Items to Deleted Items.
- You can then right mouse click on the Deleted Items folder and select Empty "Deleted Items" Folder. When you answer, "Yes", all of the messages will be deleted. Of course, you can do this at any time as well.
- If you want to permanently delete messages automatically, choose Options from the Tools menu and then check the Empty the Deleted Items Folder Upon Exiting box. Then, whenever you exit Outlook, the Deleted Items folder will be emptied.

For additional methods, consult any good book on Microsoft Outlook, or call the HelpDesk at extension 4357 (HELP) from on-campus or (915) 747-5257 from off-campus for assistance or to register for training on MS Outlook.

Revision History:
First Draft: April 27, 2005
Revised: June 22, 2007
Revised: September 26, 2007
Revised: May 31, 2011

E-mail for Retirees

1.0 Policy

It is the policy of the University to offer all retirees the opportunity to retain their University-sponsored e-mail account. This policy is established to achieve the following:

- Define an employee's eligibility to maintain an e-mail account as a Retiree;
- Identify the responsibilities of the Retiree who is assigned an e-mail account; and,
- Outline procedures for Retirees on the method for requesting and maintaining e-mail accounts.

2.0 Purpose and Scope

The purpose of this policy is to establish the guidelines for maintaining e-mail accounts at UTEP.

This policy applies to all retirees of The University of Texas at El Paso. For purposes of this policy, a "retiree" is defined as an individual who participates in the uniform group benefits program provided by UT System available to all retirees.

3.0 Retiree Accounts

Information regarding e-mail access to retirees will be provided by Human Resource Services (HRS) during the retirement conference between HRS and the retiree. Information about the maintenance of their e-mail account will be provided at that time.

4.0 Usage and Expiration of Accounts

All e-mail use is subject to the general policies governing use of University Information Resources. The website for this information is: http://admin.utep.edu/DesktopDefault.aspx?tabid=204.

A retiree e-mail account that is inactive for six (6) consecutive months will be closed unless the University's HelpDesk (747-5257) receives a request for extension. When an account is about to expire, an e-mail notification will be sent to the retiree informing them of their options. An account may also be closed at the written request of the retiree or in the event of the retiree's death. Upon closure, the account and its files will be removed permanently. Human Resource Services will notify the HelpDesk on this occasion via an e-mail message.

5.0 Problems with Accounts

Problems with an e-mail account should be reported to the HelpDesk. Security infractions should be reported to security@utep.edu or to the HelpDesk.

Revision History
First Draft: July 14, 2004
Revised: July 8, 2011

Sponsored E-mail Accounts

1.0 Introduction

It is necessary that the University establish provisions for providing e-mail accounts to individuals outside of the University. These accounts, normally referred to as "Sponsored" accounts, provide non-UTEP individuals with a limited amount of access to University Information Resources.

2.0 Purpose

The purpose of this policy is to establish the guidelines for creating and maintaining a sponsored e-mail account for non-UTEP personnel.

3.0 Scope

This policy applies to all accounts established for use by individuals who are not otherwise classified as faculty, staff, or students of The University of Texas at El Paso.

4.0 Policy

This policy is established to achieve the following:

- Define who is eligible for a sponsored e-mail account
- Identify the responsibilities of the recipient of a sponsored e-mail account
- Educate administrators on the method for requesting and maintaining a sponsored e-mail account.

4.1 Requesting Sponsored Accounts

The University President, Vice Presidents, Deans, Directors, or Chairs may sponsor an e-mail account for non-University personnel who are affiliated with the University and are assisting the University in meeting its mission. Requests must be made to the HelpDesk at extension 4357 (HELP) from on-campus or (915) 747-5257 from off-campus. The requestor must provide their name, employee identification number, date of birth, estimated period of time the account will be needed, and phone number. The requestor must also provide the recipient's full name, date of birth, business or home address, and phone number. Once established, the HelpDesk will contact the owner of the account with an ID and password. The name of the sponsor will be recorded along with the owner of the account for possible renewal.

4.4 Usage

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 existing University policies.

- 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.
- 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 the approval of the President or a Vice President of the University may a general broadcast message (e-mail bulletin) be placed on the e-mail system.
- The content, maintenance, and disposition or retention of e-mail messages is the responsibility of the member to whom the e-mail account or address is assigned. E-mail that conducts official business must be referred to the member's former administrative head. In order to obtain optimum efficiency and service, the system administrator of the e-mail system may delete e-mail messages older than two weeks. E-mail messages requiring retention beyond this time limit should be downloaded to disks or printed for storage by each user.
- Using email for purposes of political lobbying or campaigning.
- Violating copyright laws by inappropriately distributing protected works.
- Posing as anyone other than oneself when sending email, except when authorized to send messages for another when serving in an administrative support role.
- The use of unauthorized email software.
- Sending or forwarding email that is likely to contain computer viruses.

4.4 Expiration of Accounts

All sponsored e-mail accounts that are within the scope of this policy will expire annually. When an account is about to expire, an e-mail notification will be sent to the administrator and account owner two weeks prior to the expiration date announcing that the account will be expired. If no action is taken by the owner of the account, i.e., the HelpDesk does not receive a request for an extension, the account will be locked and any files belonging to the account will be retained for two weeks. If the HelpDesk has received no request for extension after the two-week retention period, the account and its files will be permanently removed.

In addition, a list of sponsored accounts will be emailed to sponsors each year for their review. This list is for information purposes only. If an account listed is found to no longer be necessary, the sponsor may email or phone the HelpDesk and request that it be disabled.

4.5 Problems with Accounts

Problems with a sponsored e-mail account should first be reported to the administrator of the sponsored account. If the problem cannot be resolved, the problems should be reported to

the HelpDesk at extension 4357 (HELP) from on-campus or (915) 747-5257 from off-campus. Security infractions should be reported to security@utep.edu or to the HelpDesk.

5.0 Enforcement

Violations to this policy can result in temporary or permanent loss of access to University Information Resources for the offending individual.

First Draft: May 17, 2004
Revised: June 5, 2011

Incident Management

1.0 Introduction

The number of computer security incidents and the resulting cost of business disruption and service restoration continue to escalate. Implementing solid security policies, blocking unnecessary access to networks and computers, improving user security awareness, and early detection and mitigation of security incidents are some the actions that can be taken to reduce the risk and drive down the cost of security incidents.

2.0 Purpose

This document describes the requirements for dealing with computer security incidents. Security incidents include, but are not limited to: virus, worm, and Trojan horse detection, unauthorized use of computer accounts and computer systems, as well as complaints of improper use of Information Resources as outlined in the Email Policy, the Internet Policy, and the Acceptable Use Policy.

3.0 Scope

The UTEP Incident Management Policy applies equally to all individuals that use any University Information Resources.

4.0 Policy

UTEP Critical Incident Response Team (CIRT) members have pre-defined roles and responsibilities which can take priority over normal duties.

Whenever a security incident, such as a virus, worm, hoax email, discovery of hacking tools, altered data, etc. is suspected or confirmed, the appropriate Incident Management procedures must be followed.

The ISO is responsible for notifying the IRM and the CIRT and initiating the appropriate incident management action including restoration as defined in the Incident Management Procedures.

The ISO is responsible for determining the physical and electronic evidence to be gathered as part of the Incident Investigation.

The appropriate technical resources from the CIRT are responsible for monitoring that any damage from a security incident is repaired or mitigated and that the vulnerability is eliminated or minimized where possible.

The ISO, working with the IRM, will determine if a widespread UTEP communication is required, the content of the communication, and how best to distribute the communication.

The appropriate technical resources from the CIRT are responsible for communicating new issues or vulnerabilities to the system vendor and working with the vendor to eliminate or

mitigate the vulnerability.

The ISO is responsible for initiating, completing, and documenting the incident investigation with assistance from the CIRT.

The UTEP ISO is responsible for reporting the incident to the:

- Executive Vice President
- IRM
- Department of Information Resources (DIR) as outlined in TAC §202
- Local, state or federal law officials as required by applicable statutes and/or regulations

The ISO is responsible for coordinating communications with outside organizations and law enforcement.

In the case where law enforcement is not involved, the ISO will recommend disciplinary actions, if appropriate, to the IRM.

In the case where law enforcement is involved, the ISO will act as the liaison between law enforcement and UTEP.

5.0 Disciplinary Actions

Violation of this policy may result in disciplinary action which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of University Information Resources access privileges, civil, and criminal prosecution.

Revision History
First Draft: April 2, 2002
Revised September 11, 2002
Revised July 8, 2011

Intrusion Detection

1.0 Introduction

Intrusion detection plays an important role in implementing and enforcing an organizational security policy. As information systems grow in complexity, effective security systems must evolve. With the proliferation of the number of vulnerability points introduced by the use of distributed systems some type of assurance is needed that the systems and network are secure. Intrusion detection systems can provide part of that assurance.

2.0 Purpose

Intrusion detection provides two important functions in protecting information resources:

- Feedback: information as to the effectiveness of other components of the security system. If a robust and effective intrusion detection system is in place, the lack of detected intrusions is an indication that other defenses are working.

- Trigger: a mechanism that determines when to activate planned responses to an intrusion incident.

3.0 Scope

The UTEP Intrusion Detection Policy applies to all individuals that are responsible for the installation of new Information Resources, the operations of existing Information Resources, and individuals charged with Information Resources Security.

4.0 Policy

Operating system, user accounting, and application software audit logging processes must be enabled on all host and server systems.

Alarm and alert functions of any firewalls and other network perimeter access control systems must be enabled.

Audit logging of any firewalls and other network perimeter access control system must be enabled.

Audit logs from the perimeter access control systems must be monitored/reviewed daily by the system administrator.

System integrity checks of the firewalls and other network perimeter access control systems must be performed on a routine basis.

Audit logs for servers and hosts on the internal, protected, network must be reviewed on a weekly basis. The system administrator will furnish any audit logs as requested by the ISO.

Host based intrusion tools will be checked on a routine basis.

All trouble reports should be reviewed for symptoms that might indicate intrusive activity.

All suspected and/or confirmed instances of successful and/or attempted intrusions must be immediately reported according to the Information Security Office.

Users shall be trained to report any anomalies in system performance and signs of wrongdoing to the Information Security Office or HelpDesk.

5.0 Disciplinary Actions

Violation of this policy may result in disciplinary action which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of University Information Resources access privileges, civil, and criminal prosecution.

Revision History
First Draft: April 4, 2002
Revised: September 17, 2002
Revised: July 5, 2011

Network Access

1.0 Introduction

The UTEP network infrastructure is provided as a central utility for all users of University Information Resources. It is important that the infrastructure, which includes cabling and the associated 'active equipment', continues to develop with sufficient flexibility to meet University demands while at the same time remaining capable of exploiting anticipated developments in high speed networking technology to allow the future provision of enhanced user services.

2.0 Purpose

The purpose of the UTEP Network Access Policy is to establish the rules for the access and use of the network infrastructure. These rules are necessary to preserve the integrity, availability and confidentiality of University Information Resources.

3.0 Scope

This policy applies equally to all individuals with access to any University Information Resource. Additional requirements may apply depending on applicable laws, regulations, and/or standards.

4.0 Policy

Users are permitted to use only those network addresses issued to them by the UTEP Telecommunications Infrastructure (TI) group (aka Networking group).

Remote users may connect to University Information Resources only through an ISP and using protocols approved by UTEP.

Users inside the UTEP firewall may not be connected to the UTEP network at the same time a modem is being used to connect to an external network.

Users must not extend or re-transmit network services in any way. This means you must not install a router, switch, hub, or wireless access point to the UTEP network without UTEP TI approval.

Users must not install network hardware or software that provides network services without UTEP TI approval.

Non-University computer systems that require network connectivity must conform to UTEP Information Security Policies, Standards, and Guidelines.

Users must not download, install or run security programs or utilities that reveal weaknesses in the security of a system. For example, UTEP users must not run password cracking programs, packet sniffers, network mapping tools, or port scanners while connected in any manner to the UTEP network infrastructure.

Users are not permitted to alter network hardware in any way.

5.0 Disciplinary Actions

Violation of this policy may result in disciplinary action which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of University Information Resources access privileges, civil, and criminal prosecution.

Revision History
First Draft: April 4, 2002
Revised: September 17, 2002
Revised: July 5, 2011

Network Configuration

1.0 Introduction

The UTEP network infrastructure is provided as a central utility for all users of University Information Resources. It is important that the infrastructure, which includes cabling and the associated equipment such as routers and switches, continues to develop with sufficient flexibility to meet user demands while at the same time remaining capable of exploiting anticipated developments in high speed networking technology to allow the future provision of enhanced user services.

2.0 Purpose

The purpose of the UTEP Network Configuration Policy is to establish the rules for the maintenance, expansion and use of the network infrastructure. These rules are necessary to preserve the integrity, availability, and confidentiality of UTEP information.

3.0 Scope

The UTEP Network Configuration Policy applies equally to all individuals with access to any University Information Resource. Additional requirements may apply depending on applicable laws, regulations, and/or standards.

4.0 Policy

The UTEP Telecommunications Infrastructure (TI) group is solely responsible for the UTEP network infrastructure and will continue to manage further developments and enhancements to this infrastructure.

To provide a consistent UTEP network infrastructure capable of exploiting new networking developments, all cabling must be installed by UTEP TI or an approved contractor.

All network connected equipment must be configured to a specification approved by UTEP TI.

All hardware connected to the UTEP network is subject to UTEP TI management and monitoring standards.

Changes to the configuration of active network management devices must not be made without the approval of UTEP TI.

The UTEP network infrastructure supports a well-defined set of approved networking protocols. Any use of non-sanctioned protocols must be approved by UTEP TI.

The networking addresses for the supported protocols are allocated, registered and managed centrally by UTEP TI.

All connections of the network infrastructure to external third party networks are the

responsibility of UTEP TI. This includes connections to external telephone networks.

UTEP TI Firewalls must be installed and configured in accordance with the UTEP Firewall Implementation Standard documentation.

The use of departmental firewalls is not permitted without the written authorization from UTEP TI.

Users must not extend or re-transmit network services in any way. This means you must not install a router, switch, hub, or wireless access point to the UTEP network without UTEP TI approval.

Users must not install network hardware or software that provides network services without UTEP TI approval.

Users are not permitted to alter network hardware in any way.

5.0 Disciplinary Actions

Violation of this policy may result in disciplinary action which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of University Information Resources access privileges, civil, and criminal prosecution.

Revision History
First Draft: April 3, 2002
Revised: September 17, 2002
Revised: July 5, 2011

Passwords

1.0 Introduction

User authentication is a means to control who has access to a University Information Resource. Access gained by an unauthorized person may cause loss of information confidentiality, integrity and availability that may further result in loss of revenue, liability, loss of trust, or embarrassment to UTEP.

Three factors, or a combination of these factors, can be used to authenticate a user. Examples are:

- Something you know - password, Personal Identification Number (PIN)
- Something you have - Smartcard or token.
- Something you are - fingerprint, iris scan, voice.

Until other methods are added at the University, the sole method of authentication will most likely be a password. It is therefore incumbent upon you, the user, to choose a strong password to protect yourself and the University.

2.0 Purpose

The purpose of the UTEP Password Policy is to establish the rules for the creation, distribution, safeguarding, termination, and reclamation of the UTEP user authentication mechanisms.

3.0 Scope

This policy applies equally to all individuals who use any University Information Resources.

4.0 Policy

4.1 Passwords

All passwords, including initial passwords, must be constructed and implemented according to the following rules:

Passwords must

- Your password must be between 8 and 20 characters in length.
- You may not re-use any of your last 4 passwords.
- Your password must contain letters, numbers, and special characters. The special characters that are permitted are ! @ # $ % & * ( ) - + = , < > : ; " ' ..
- Your password cannot contain any words found in our dictionary or common proper nouns of four letters or longer. In addition, common letter transpositions are not allowed (for example @ for a, ! for i, or zero for O).
- Your password cannot contain your first or last name.
- Your password cannot contain your birthday in any form.

- Your password cannot contain your Social Security Number.
- Administrators must have a password a minimum length of 17 characters.

All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed annually.

Administrator passwords must be changed at least every 90-Days.

4.2 Pass Phrases

Pass phrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the pass phrase to "unlock" the private key, the user cannot gain access.

Pass phrases are not the same as passwords. A pass phrase is a longer version of a password and is, therefore, more secure. A pass phrase is typically composed of multiple words. Because of this, a pass phrase is more secure against "dictionary attacks."

A good pass phrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good pass phrase:

"The*?#>*@TrafficOnThe101Was*&#!#ThisMorning"

All of the rules above that apply to passwords apply to pass phrases.

5.0 Password Security

User account passwords must not be divulged to anyone. UTEP IT and IT contractors will not ask for user account passwords. If someone demands a password, refer them to this document or have them call someone in the Information Security Office.

Security tokens (i.e. Smartcard) must be returned on demand or upon termination of the relationship with UTEP.

If the security of a password is in doubt, the password must be changed immediately.

Computing devices must not be left unattended without enabling a password-protected screensaver or logging-off of the device.

Do not use the "Remember Password" feature of applications (e.g., Eudora, OutLook, and Netscape Messenger).

Do not write passwords down and store them anywhere in your office.

Do not store unencrypted passwords in a file on ANY computer system (including Palm Pilots or similar devices).

If an account or password is suspected of having been compromised, report the incident to

the Information Security Office and change all passwords immediately.

HelpDesk password change procedures must include the following:

- Authenticate the user to the HelpDesk before changing password.
- Change to a strong password.
- The user must change password at first login.

In the event passwords are found or discovered, the following steps must be taken:

- Take control of the passwords and protect them.
- Report the discovery to the UTEP HelpDesk.
- Transfer the passwords to an authorized person as directed by the UTEP Information Security Officer.

User accounts that have system-level privileges granted through group memberships or programs such as "sudo" must have a unique password from all other accounts held by that user. Passwords must conform to the administrator-level requirements and must be changed at least every 90-days (see 4.1 above).

Passwords must not be inserted into email messages or other forms of electronic communication. Where SNMP is used, the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).

Password cracking or guessing may be performed on a periodic or random basis by the Information Security Office or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it.

6.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Revision History
First Draft: March 28, 2002
Revised: April 3, 2002
Revised: September 19, 2002
Revised: April 7, 2003
Revised: June 18, 2003
Revised: August 4, 2006
Revised: September 11, 2006
Revised: July 26, 2011
Revised: September 30, 2014
Revised: December 9, 2016 – reflect annual user password change requirement

Personnel Procedures

Positions of Special Trust:

Managers should review, annually, the duties of personnel under their supervision, or upon job description change, to determine if the position is one of special trust.

Security and Training:

Personnel whose duties bring them into contact with confidential information will be required to attend an awareness and training program at least annually and will receive periodic briefings. As appropriate, annual training programs will include such topics as:

- Public access to information.
- Policy against using university resources for personal purposes.
- Disposal of confidential information.
- Protection of passwords.
- Message authentication and data encryption.
- Privacy and confidentiality.
- Copyright protection and the use of copyrighted material.
- Work habits in relation to security.

Hiring and Termination Procedures

Policies and procedures regarding the use and security of University Information Resources will be communicated to new employees. Additionally, new employees will be required to sign a Acceptable Use Policy Form, to signify that they have read and received a copy of that policy and that they will comply with the policies therein.

Applicants for employment for a position classified as security-sensitive are subject to a criminal history record check pursuant to Section 51.215, Texas Education Code and approved institutional policy on security-sensitive positions.

Each employee's information access authority will be reviewed periodically including review at time of a transfer, promotion, or termination.

Passwords for consultants and contractors will be disabled at the end of their contract.

Revision History:
First Draft: April 27, 2005
Revised: July 26, 2011

Physical Access

1.0 Introduction

Technical support staff, security administrators, system administrators, and others may have Information Resource physical facility access requirements as part of their function. The granting, controlling, and monitoring of the physical access to Information Resources facilities is extremely important to an overall security program.

2.0 Purpose

The purpose of the UTEP Physical Access Policy is to establish the rules for the granting, control, monitoring, and removal of physical access to Information Resource facilities.

3.0 Scope

The UTEP Physical Access Policy applies to all individuals within the UTEP enterprise that are responsible for the installation and support of Information Resources, individuals charged with Information Resources Security and data owners.

4.0 Policy

All physical security systems must comply with all applicable regulations such as, but not limited to, building codes and fire prevention codes.

Physical access to all Information Resources restricted facilities must be documented and managed.

All Information Resources facilities must be physically protected in proportion to the criticality or importance of their function at UTEP.

Access to Information Resources facilities must be granted only to UTEP support personnel and contractors, whose job responsibilities require access to that facility.

The process for granting card and/or key access to Information Resources facilities must include the approval of the person responsible for the facility.

Each individual that is granted access rights to an Information Resources facility must receive emergency procedures training for the facility and must sign the appropriate access and non-disclosure agreements.

Requests for access must come from the applicable UTEP data/system owner.

Access cards and/or keys must not be shared or loaned to others.

Access cards and/or keys that are no longer required must be returned to the person responsible for the Information Resources facility. Cards must not be reallocated to another individual bypassing the return process.

Lost or stolen access cards and/or keys must be reported to the person responsible for the Information Resources facility.

Cards and/or keys must not have identifying information other than a return mail address.

All Information Resources facilities that allow access to visitors will track visitor access with a sign in/out log.

A service charge may be assessed for access cards and/or keys that are lost, stolen or are not returned.

Card access records and visitor logs for Information Resources facilities must be kept for routine review based upon the criticality of the Information Resources being protected.

The person responsible for the Information Resources facility must remove the card and/or key access rights of individuals that change roles within UTEP or are separated from their relationship with UTEP.

Visitors must be escorted in card access controlled areas of Information Resources facilities.

The person responsible for the Information Resources facility must review access records and visitor logs for the facility on a periodic basis and investigate any unusual access.

The person responsible for the Information Resources facility must review card and/or key access rights for the facility on a periodic basis and remove access for individuals that no longer require access.

Signage for restricted access rooms and locations must be practical, yet minimal discernible evidence of the importance of the location should be displayed.

5.0 Disciplinary Actions

Violation of this policy may result in disciplinary action which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of UTEP Information Resources access privileges, civil, and criminal prosecution.

Revision History
First Draft: April 3, 2002
Revised: September 11, 2002
Revised: September 19, 2002
Revised: July 26, 2011

Portable Computing

1.0 Introduction

Portable computing devices are becoming increasingly powerful and affordable. Their small size and functionality are making these devices ever more desirable to replace traditional desktop devices in a wide number of applications. However, the portability offered by these devices may increase the security exposure to groups using the devices.

2.0 Purpose

The purpose of the UTEP Portable Computing Security Policy is to establish the rules for the use of mobile computing devices and their connection to the network. These rules are necessary to preserve the integrity, availability, and confidentiality of UTEP Information Resources.

3.0 Scope

The UTEP Portable Computing Security Policy applies equally to all individuals that utilize Portable Computing devices and access UTEP Information Resources.

4.0 Policy

Only UTEP approved portable computing devices may be used to access UTEP Information Resources.

Portable computing devices must be password protected.

UTEP data should not be stored on portable computing devices. However, in the event that there is no alternative to local storage, all confidential UTEP data must be encrypted using approved encryption techniques.

UTEP data must not be transmitted via wireless to or from a portable computing device unless approved wireless transmission protocols, along with approved encryption techniques, are utilized.

Non-UTEP computer systems that require network connectivity must conform to UTEP Information Security Policies and Standards, and must be approved by the UTEP Information Security Office by submitting a Service Desk Request (please contact the HelpDesk for assistance).

Unattended portable computing devices must be physically secure. This means they must be locked in an office, locked in a desk drawer or filing cabinet, or attached to a desk or cabinet via a cable lock system.

5.0 Disciplinary Actions

Violation of this policy may result in disciplinary action which may include termination for

employees and temporaries; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of UTEP Information Resources access privileges, civil, and criminal prosecution.

Revision History
First Draft: April 4, 2002
Revised: September 19, 2002
Revised: July 26, 2011

Information Service Privacy

1.0 Introduction

Privacy Policies are mechanisms used to establish the limits and expectations for the users of UTEP Information Resources. UTEP IR users should have no expectation of privacy with respect to Information Resources except as otherwise provided by applicable privacy laws or unless expressly stated by Regent's Rules.

2.0 Purpose

The purpose of the UTEP Information Services Privacy Policy is to clearly communicate the UTEP Information Services Privacy expectations to Information Resources users.

3.0 Scope

The UTEP Information Services Privacy Policy applies to all individuals who use UTEP Information Resources.

4.0 Policy

4.1 General

Electronic files created, sent, received, or stored on IR owned, leased, administered, or otherwise under the custody and control of UTEP are not private and may be accessed by UTEP ISO employees at any time without knowledge of the IR user or owner for the purpose of system administration and maintenance, for resolution of technical problems, for compliance with the Texas Public Information Act, for compliance with federal and state subpoenas, court orders, or other written authorizations, to conduct the business of the university, and to perform audits.

To manage systems and enforce security, UTEP may log, review, and otherwise utilize any information stored on or passing through its IR systems in accordance with the provisions and safeguards provided in the Texas Administrative Code (TAC) S202. UTEP may also capture user activity such as telephone numbers dialed and web sites visited.

A wide variety of third parties have entrusted their information to UTEP for business purposes, and all workers at UTEP must do their best to safeguard the privacy and security of this information. The most important of these third parties is the individual customer; customer account data is accordingly confidential and access will be strictly limited based on business need for access.

Users must report any weaknesses in UTEP computer security, any incidents of possible misuse or violation of this agreement to the proper authorities by contacting the appropriate management or the Information Security Office.

Users must not attempt to access any data or programs contained on UTEP systems for which they do not have authorization or explicit consent.

4.2 Public Access Privacy Policy

UTEP web sites available to the general public must contain a Privacy Statement. An example of a good public Privacy Statement follows:

Web site Privacy Statement on the Use of Information Gathered from the General Public

The following statement applies only to members of the general public and is intended to address concerns about the types of information gathered from the public, if any, and how that information is used.

5.0 Disciplinary Actions

Violation of this policy may result in disciplinary action which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of UTEP Information Resources access privileges, civil, and criminal prosecution.

Revision History
First Draft: April 3, 2002
Revised: September 19, 2002
Revised: July 29, 2003
Revised: July 26, 2011

Remote Access

1.0 Purpose

The purpose of this policy is to define standards for connecting to The University of Texas at El Paso's (UTEP) network from any host. These standards are designed to minimize the potential exposure to the university from damages which may result from unauthorized use of UTEP resources. Damages include the loss of university confidential data, intellectual property, damage to public image, damage to critical UTEP internal systems, etc.

2.0 Scope

This policy applies to all UTEP Information Resources users (e.g., employees, students, contractors, vendors, agents, guests, etc.) who access university resources with any device whether university-owned or personally owned.

Remote access implementations that are covered by this policy include, but are not limited to, frame relay, ISDN, DSL, VPN, SSH, cable modems, etc.

3.0 Policy

3.1 General

It is the responsibility of UTEP Information Resources users with remote access privileges to the university resources to ensure that their remote access connection is given the same consideration as the user's on-site connection.

By using UTEP Information Resources, users agree to bear the responsibility for the consequences should the access be misused.

Please review the following policies for details of protecting information when accessing the network via remote access methods, and acceptable use of The University of Texas at El Paso's network:

- Acceptable Encryption Policy
- Acceptable Use Policy
- Virtual Private Network (VPN) Policy
- Wireless Communications Policy

3.2 Requirements

Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication or public/private keys with strong pass-phrases. For information on creating a strong pass-phrase see the Password Policy.

At no time should any University of Texas at El Paso employee provide their login or email password to anyone, not even family members.

Users with remote access privileges must ensure that their University of Texas at El Paso-owned or personal computer, workstation or device, which is remotely connected to UTEP Information Resources, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.

Users with remote access privileges to UTEP Information Resources (e.g., network, etc.) must not use non-UTEP email accounts (i.e., Hotmail, Yahoo, AOL, etc.), or other external resources to conduct university business; thereby ensuring that official business is never confused with personal business, and that university information/information resources are not placed at risk.

Routers for dedicated ISDN lines configured for access to UTEP Information Resources must meet minimum authentication requirements of CHAP.

Reconfiguration of a home user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time.

Frame Relay must meet minimum authentication requirements of DLCI standards. Non-standard hardware configurations must be approved by Remote Access Services, and the Information Security Office (ISO) must approve security configurations for access to hardware.

All hosts that connect to UTEP Information Resources via remote access technologies must have an anti-virus software installed and enabled. Anti-virus software should be configured to update the signatures or definitions daily. Additionally, the firewall should be enabled. Note that these requirements also apply to personal computers. Third party connections must comply with requirements as stated in the Third Party Agreement.

Personal equipment that is used to connect to University Information Resources must meet the same requirements of university-owned equipment for remote access.

Organizations or individuals wishing to implement non-standard Remote Access solutions on University Information Resources must obtain prior approval from the Information Security Office (ISO) and execute an Acceptable Use Agreement or Third Party Agreement.

4.0 Enforcement

Violation of this policy may result in disciplinary action which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of UTEP Information Resources access privileges, civil, and criminal prosecution.

Revision History
First Draft: April 1, 2002
Revised: September 19, 2002
Revised: November 18, 2003
Revision: October 17, 2011

Risk Assessment

1.0 Purpose

To empower the Information Security Office (ISO) to perform periodic information security risk assessments (RAs) for the purpose of determining areas of vulnerability, and to initiate appropriate remediation.

2.0 Scope

Risk assessments can be conducted on any entity within The University of Texas at El Paso (UTEP) or any outside entity that has signed a Third Party Agreement with UTEP. Risk assessments can be conducted on any information system, to include applications, servers, and networks, and any process or procedure by which these systems are administered and/or maintained.

3.0 Policy

The execution, development and implementation of remediation programs are the joint responsibility of the ISO and the department responsible for the systems area being assessed. Employees are expected to cooperate fully with any risk assessment being conducted on systems for which they are held accountable. Employees are further expected to work with the ISO Risk Assessment Team in the development of a remediation plan.

4.0 Enforcement

Violation of this policy may result in disciplinary action which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of UTEP Information Resources access privileges, civil, and criminal prosecution.

Revision History
First Draft: April 1, 2002
Revised: September 19, 2002
Revised: October 19, 2011

Router Security

1.0 Purpose

This document describes a required minimal security configuration for all routers and switches connecting to a production network or used in a production capacity at or on behalf of The University of Texas at El Paso (UTEP).

2.0 Scope

All routers and switches connected to UTEP production networks are affected. Routers and switches within internal, secured labs are not affected. Routers and switches within DMZ areas fall under the Internet DMZ Equipment Policy.

3.0 Policy

Every router must meet the following configuration standards:

- No local user accounts are configured on the router. Routers must use RADIUS or TACACS+ for all user authentications.
- The enable password on the router must be kept in a secure encrypted form. The router must have the enable password set to the current production router password from the router's support organization. Vendor provided passwords must be changed to meet UTEP’s minimum password requirements.
- Disallow the following:
    - IP directed broadcasts
    - Incoming packets at the router sourced with invalid addresses such as RFC1918 address
    - TCP small services
    - UDP small services
    - All source routing
    - All web services running on router
- Use University standardized SNMP community strings.
- Access Control List (ACL) rules are to be added as business needs arise.
- The router must be included in the university enterprise management system with a designated point of contact.
- Each router must have the following statement posted in clear view: "UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED. You must have explicit permission to access or configure this device. All activities performed on this device may be logged, and violations of this policy may result in disciplinary action, and may be reported to law enforcement. There is no right to privacy on this device."

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Revision History
First Draft: April 1, 2002
Revised: September 19, 2002
Revised: December 15, 2011

Security Monitoring

1.0 Introduction

Security Monitoring is a method used to confirm that the security practices and controls in place are being adhered to and are effective. Monitoring consists of activities such as, but not limited to, the review of:

- Automated intrusion detection/prevention system logs
- Firewall logs
- User account logs
- Network scanning logs
- Application logs
- Data backup recovery logs
- Service Desk Requests
- Other log and error files.

2.0 Purpose

The purpose of the Security Monitoring Policy is to ensure that Information Resource security controls are in place, are effective, and are not being bypassed. One of the benefits of security monitoring is the early identification of security issues or new security vulnerabilities. This early identification can help to prevent a security issue or vulnerability before harm can be done, or to minimize the potential impact. Other benefits include Audit Compliance, Service Level Monitoring, Performance Measuring, Limiting Liability, and Capacity Planning.

3.0 Scope

The UTEP Security Monitoring Policy applies to all individuals that are responsible for the installation of new Information Resources, the operations of existing Information Resources, and individuals charged with Information Resource Security.

4.0 Policy

Automated tools will provide real time notification of detected security issues and vulnerability exploitation. Where possible a security baseline will be developed and the tools will report exceptions. These tools will be deployed to monitor:

- Internet traffic
- Electronic mail traffic
- LAN traffic, protocols, and device inventory
- Operating system security parameters including security software

The following files will be checked for signs of security issues and vulnerability exploitation at a frequency determined by risk:

- Automated intrusion detection system logs
- Firewall logs

- User account logs
- Network scanning logs
- System error logs
- Application logs
- Data backup and recovery logs
- HelpDesk trouble tickets
- Telephone activity - Call Detail Reports
- Network printer and fax logs

The following checks will be performed at least annually by assigned individuals:

- Password strength
- Unauthorized network devices
- Unauthorized personal web servers
- Unsecured sharing of devices
- Unauthorized modem use
- Operating System and Software Licenses

Any security issues discovered will be reported to the ISO for follow-up investigation.

5.0 Disciplinary Actions

Violation of this policy may result in disciplinary action which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of UTEP Information Resources access privileges, civil, and criminal prosecution.

Revision History
First Draft: April 4, 2002
Revised: September 19, 2002
Revised: December 13, 2011

Security Training

1.0 Introduction

Understanding the importance of computer security and individual responsibilities and accountability for computer security are paramount to achieving organization security goals. This can be accomplished with a combination of general computer security awareness training and targeted, product specific training. The philosophy of protection and specific security instructions needs to be taught to, and re-enforced with, computer users. The security awareness and training information needs to be continuously upgraded and reinforced.

2.0 Purpose

The purpose of the Security Training Policy is to describe the requirements for ensuring each user of UTEP Information Resources is receiving adequate training on computer security issues.

3.0 Scope

The UTEP Security Training Policy applies equally to all individuals that use any UTEP Information Resources.

4.0 Policy

All new users must attend an approved Security Awareness training class prior to, or at least within 30 days of, being granted access to any UTEP Information Resources.

All users must sign an acknowledgment stating they have read and understand UTEP requirements regarding computer security policies and procedures.

All users (employees, consultants, contractors, temporaries, etc.) must be provided with sufficient training and supporting reference materials to allow them to properly protect UTEP Information Resources.

The ISO must prepare, maintain, and distribute one or more information security manuals that concisely describe UTEP Information Security Policies and Procedures.

All users must receive annual computer security compliance training.

The ISO must develop and maintain a communications process to be able to communicate new computer security program information, security bulletin information, and security items of interest.

5.0 Disciplinary Actions

Violation of this policy may result in disciplinary action which may include termination for employees and temporaries; a termination of employment relations in the case of contractors

or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of UTEP Information Resources access privileges, civil, and criminal prosecution.

Revision History
First Draft: April 4, 2002
Revised: September 12, 2003
Revised: December 13, 2011

Server Hardening

1.0 Introduction

Servers are depended upon to deliver data in a secure, reliable fashion. There must be assurance that data confidentiality, integrity, and availability (C-I-A) is maintained and that security controls are proportional to the requirements of the data processed by the system (i.e., Category I, Category II, Category III, PCI, etc.). One of the required steps to attain this assurance is to ensure that the servers are installed and maintained in a manner that prevents unauthorized access, unauthorized use, and no disruptions in service, with particular focus on configuration issues.

2.0 Purpose

The purpose of the UTEP Server Hardening Policy document is to describe the requirements for installing a new server in a secure fashion and maintaining the security integrity of the server and application software.

3.0 Scope

The UTEP Server Hardening Policy applies to all individuals that are responsible for the installation of new Information Resources, the operations of existing Information Resources, and individuals charged with Information Resource Security.

4.0 Policy

A server must be protected and not be connected to the UTEP network until it is in a UTEP ISO accredited secure state and the network connection is approved by the ISO. For more information and additional requirements please refer to The University of Texas at El Paso Information Security Minimum Security Standards for Systems and The University of Texas at El Paso ISO Minimum Security Standards for Payment Card Industry (PCI) Data Security Standard (DSS).

The Minimum Security Standards for Systems provides the detailed information required to harden a server and must be implemented for UTEP ISO accreditation. Some of the general steps in this standard include, but are not limited to:

- Installing the operating system from an IS approved source
- Applying vendor supplied patches
- Anti-Virus software must be installed and enabled
- Removing unnecessary software, accounts, system services, and drivers
- Setting security parameters, file protections, firewall, and enabling audit logging
- Disabling or changing the password of default accounts
- Insure appropriate permissions are granted on the system as well as any share folders

The ISO will monitor security issues, both internal to UTEP and externally. The ISO or other approved team will manage the release of security patches on behalf of UTEP.

The ISO or other approved team will test security patches against IS core resources before release where practical, and not more than 30 days from release date for PCI systems; the only exception being when immediate application would interfere with business requirements.

Security patches must be implemented within the specified timeframe of notification from the ISO.

5.0 Disciplinary Actions

Violation of this policy may result in disciplinary action which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of UTEP Information Resources access privileges, civil, and criminal prosecution.

Revision History
First Draft: April 4, 2002
Revised: September 19, 2002
Revised: December 19, 2011

Server Security

1.0 Purpose

The purpose of this policy is to establish standards for the base configuration of internal server equipment that is owned and/or operated by The University of Texas at El Paso. Effective implementation of this policy will minimize unauthorized access to University confidential, PCI, proprietary, and other information and technology.

2.0 Scope

This policy applies to server equipment owned and/or operated by The University of Texas at El Paso, and to servers registered under any UTEP-owned internal network domain.

This policy is specifically for equipment on the internal UTEP network.

3.0 Policy

This policy is to ensure that servers owned/operated, deployed, configured, and managed meet the security requirements of UTEP. For more information and additional requirements please refer to The University of Texas at El Paso Information Security Minimum Security Standards for Systems and The University of Texas at El Paso ISO Minimum Security Standards for Payment Card Industry (PCI) Data Security Standard (DSS).

3.1 Ownership and Responsibilities

All internal servers deployed at UTEP must be owned by an operational group that is responsible for system administration. Approved server configuration guides must be established and maintained by each operational group, based on business needs and approved by the Information Security Office (ISO). Operational groups should monitor configuration compliance and implement an exception policy tailored to their environment. Each operational group must establish a process for changing the configuration guides, which includes review and approval by the ISO. Servers will be classified, secured, and protected by data stewards/owners, IT owners and custodians accordingly based on the highest level of data residing on the system.

Servers that are to be physically located in IT Data Center facilities must be registered within the University Enterprise Computing Group. Servers not going into IT Data Center facilities must be registered with the ISO. At a minimum, the following information is required to identify the point of contact(s) and system administrator(s):

- Server contact(s) and backup contact
- System Administrator
- Physical location of System
- Hardware and Operating System/Version
- Main functions and applications, if applicable
- IP and MAC Address, and System Name
- UTEP Inventory Tag Number
- Specify the highest level of data (Cat I, II, III, or PCI) that will be hosted on the system

Information in the University Enterprise Management System must be kept up-to-date.

Configuration changes for production servers must follow the appropriate Change Management Guidelines.

3.2 General Configuration Guidelines

Operating System configuration should be in accordance with approved Information Security guidelines.

Services, applications, and network protocols that will not be used must be disabled where practical.

Access to services should be logged and/or protected through access-control methods such as IP Tables, Windows Firewall, etc., if possible.

The most recent security patches must be installed on the system as soon as practical, and not more than 30 days from release date for PCI systems; the only exception being when immediate application would interfere with business requirements.

Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication will do.

Always use standard security principles of least required access to perform a function. Do not use root when a non-privileged account will do.

If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or IPSec).

Servers should be physically located in an access-controlled environment.

Servers are specifically prohibited from operating from uncontrolled areas (e.g., cubicles, under desks, etc.).

3.3 Monitoring

All security-related events on critical or confidential systems must be logged and audit trails saved as follows:

- All security (most important), system and application related logs will be retained online for a minimum of 14 days.
- Daily incremental tape backups will be retained for at least 1 month.
- Weekly full tape backups of logs will be retained for at least 1 month.
- Backups must be verified at least monthly, either through automated verification, through customer restores, or through trial restores.
- Monthly full backups will be retained for a minimum of 90 days.

Security-related events will be reported to the Information Security Office, which will review logs and report incidents as appropriate. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:

- Port-scan attacks
- Evidence of unauthorized access to privileged accounts
- Anomalous occurrences that are not related to specific applications on the host.

3.4 Compliance

Audits will be performed on a regular basis by authorized organizations within UTEP.

Audits will be managed by the internal audit group or the Information Security Office (ISO), in accordance with the Audit Policy. The ISO will filter findings not related to a specific operational group and then present the findings to the appropriate support staff for remediation or justification.

Every effort will be made to prevent audits from causing operational failures or disruptions.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

SERVER: For purposes of this policy, a Server is defined as an internal University of Texas at El Paso Server. Desktop machines and Lab equipment are not relevant to the scope of this policy.

Revision History
First Draft: April 1, 2002
Revised: September 19, 2002
Revised: January 2, 2012

Software Licensing

1.0 Introduction

End-user license agreements are used by software and other information technology companies to protect their valuable intellectual assets and to advise technology users of their rights and responsibilities under intellectual property and other applicable laws.

2.0 Purpose

The purpose of the Software Licensing Policy is to establish the rules for licensed software use on UTEP Information Resources which will be in accordance with the applicable software license. Unauthorized or unlicensed use of software is regarded as a serious violation subject to disciplinary action and any such use is without the consent of the University.

3.0 Scope

This policy applies equally to all individuals that use any UTEP Information Resources.

4.0 Policy

UTEP provides a sufficient number of licensed software such that workers can get their work done in an expedient and effective manner. Management must make appropriate arrangements with the involved vendor(s) for additional licensed copies if and when additional copies are needed for business activities.

Systems administrators have the right to remove such information and software unless the involved users can provide proof of authorization from the rightful owner(s).

All departments or individuals managing university-owned systems will periodically audit all computers to inventory and document all installed software.

All departments are responsible for the accurate accounting of software purchased by the department and must ensure that the installation of the software complies with the license agreement of the software. For audit purposes, departments must maintain proof of purchase and/or original installation media for each software package. Third-party software in the possession of UTEP must not be copied unless such copying is consistent with relevant license agreements and prior management approval of such copying has been obtained, or copies are being made for contingency planning purposes.

5.0 Disciplinary Actions

Violation of this policy may result in disciplinary action which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of UTEP Information Resources access privileges, civil, and criminal prosecution.

Revision History
First Draft: April 4, 2002
Reviewed: January 12, 2012

Vendor Access

1.0 Introduction

Vendors play an important role in the support of hardware and software management, and operations for customers. Vendors can remotely view, copy and modify data and audit logs, they correct software and operating systems problems, they can monitor and fine tune system performance, they can monitor hardware performance and errors; they can modify environmental systems, and reset alarm thresholds. Setting limits and controls on what can be seen, copied, modified, and controlled by vendors will eliminate or reduce the risk of loss of revenue, liability, loss of trust, and embarrassment to UTEP.

2.0 Purpose

The purpose of the UTEP Vendor Access Policy is to establish the rules for vendor access to UTEP Information Resources and support services (A/C, UPS, PDU, fire suppression, etc.), vendor responsibilities, and protection of UTEP information.

3.0 Scope

This policy applies to all individuals that are responsible for the installation of new Information Resources assets, and the operations and maintenance of existing Information Resources and who do or may allow vendor access for maintenance, monitoring and troubleshooting purposes.

4.0 Policy

Vendors must comply with all applicable UTEP policies, practice standards and agreements, including, but not limited to:

- Acceptable Use Policies
- Auditing Policies
- Privacy Policies
- Safety Policies
- Security Policies
- Software Licensing Policies
- Non-Disclosure Agreement

Vendor agreements and contracts must specify:

- The UTEP information the vendor should have access to
- How UTEP information is to be protected by the vendor
- Acceptable methods for the return, destruction or disposal of UTEP information in the vendor's possession at the end of the contract

The Vendor must only use UTEP information and Information Resources for the purpose of the business agreement.

Any other UTEP information acquired by the vendor in the course of the contract cannot be used for the vendor's own purposes or divulged to others.

UTEP will provide an Information Security Office point of contact for the Vendor. The point of contact will work with the Vendor to make certain the Vendor is in compliance with these policies.

Each vendor must provide UTEP with a list of all employees working on the contract. The list must be updated and provided to UTEP within 24 hours of staff changes.

Each on-site vendor employee must acquire a UTEP identification badge that will be displayed at all times while on UTEP premises. The badge must be returned to UTEP when the employee leaves the contract or at the end of the contract.

Each vendor employee with access to UTEP confidential information must be cleared to handle that information.

Vendor personnel must report all security incidents directly to the appropriate UTEP personnel.

If vendor management is involved in UTEP security incident management the responsibilities and details must be specified in the contract.

Vendor must follow all applicable UTEP change control processes and procedures.

Regular work hours and duties will be defined in the contract. Work outside of defined parameters must be approved in writing by appropriate UTEP management.

All vendor maintenance equipment on the UTEP network that connects to the outside world via the network, telephone line, or leased line, and all UTEP IR vendor accounts will remain disabled except when in use for authorized maintenance.

Vendor access must be uniquely identifiable and password management must comply with the UTEP Password Practice Standard and Admin/Special Access Practice Standard. Vendor's major work activities must be entered into a log and available to UTEP management upon request. Logs must include, but are not limited to, such events as personnel changes, password changes, project milestones, deliverables, and arrival and departure times.

Upon departure of a vendor employee from the contract for any reason, the vendor will ensure that all confidential information is collected and returned to UTEP or destroyed within 24 hours.

Upon termination of contract or at the request of UTEP, the vendor will return or destroy all UTEP information and provide written certification of that return or destruction within 24 hours.

Upon termination of contract or at the request of UTEP, the vendor must surrender all UTEP Identification badges, access cards, equipment and supplies immediately. Equipment and/or supplies to be retained by the vendor must be documented by authorized UTEP

management.

Vendors are required to comply with all State and UTEP auditing requirements, including the auditing of the vendor's work.

All software used by the vendor in providing service to UTEP must be properly inventoried and licensed.

5.0 Disciplinary Actions

Violation of this policy may result in disciplinary action which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of UTEP Information Resources access privileges, civil, and criminal prosecution.

Revision History
First Draft: April 4, 2002
Revised: September 19, 2002
Revised: September 10, 2003
Revised: January 12, 2012

Virtual Private Network (VPN)

1.0 Purpose

The purpose of the Virtual Private Network (VPN) Policy is to provide guidelines for Remote Access IPSec or L2TP Virtual Private Network (VPN) connections to The University of Texas at El Paso (UTEP) Information Resources.

2.0 Scope

This policy applies to any individual (e.g, employee, contractor, consultant, temporary, and other workers including all personnel affiliated with third parties) utilizing VPNs to access UTEP Information Resources. .

3.0 Policy

Approved individuals may utilize the benefits of VPN, which are a "user managed" service. This means that the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, and paying associated fees if applicable. Further details and requirements may be found in the Remote Access Policy.

Additionally, it is the responsibility of individuals with VPN privileges to ensure that unauthorized users are not allowed access to UTEP Information Resources or their user name and password.

When actively connected to the University network, VPN will force all traffic to and from the system over the VPN tunnel: all other traffic will be dropped.

Dual (split) tunneling is NOT permitted; only one network connection is allowed. VPN gateways will be set up and managed by UTEP network operational groups.

All systems that connect to UTEP Information Resources via VPN or any other technology must have a anti-virus software installed and enabled. Anti-virus software should be configured to update signatures or definitions daily. Additionally, the firewall should be enabled. Note that these requirements also apply to personal computers. Users should contact the HelpDesk for further information about anti-virus software.

VPN users with periods of inactivity will be automatically disconnected from UTEP's network. The user must then logon again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.

Only VPN clients approved by the Information Security Office may be used.

By using VPN technology with personal equipment, users must understand that their systems are a de facto extension of UTEP's network, and as such are subject to the same rules and regulations that apply to University of Texas at El Paso-owned equipment, i.e., their machines must be configured to comply with the Office of Information Security's Security Policies.

4.0 Enforcement

Violation of this policy may result in disciplinary action which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of UTEP Information Resources access privileges, civil, and criminal prosecution.

Revision History
First Draft: April 1, 2002
Revised: September 19, 2002
Revised: September 10, 2003
Revised: January 23, 2012

Virus Protection

1.0 Introduction

The number of computer security incidents and the resulting cost of business disruption and service restoration continue to escalate. Implementing solid security policies, blocking unnecessary access to networks and computers, improving user security awareness, and early detection and mitigation of security incidents are some of the actions that can be taken to reduce the risk and drive down the cost of security incidents.

2.0 Purpose

The purpose of the Virus Protection Policy is to describe the requirements for dealing with computer virus, worm and Trojan Horse prevention, detection and cleanup.

3.0 Scope

This policy applies equally to all individuals that use any UTEP Information Resources.

4.0 Policy

All systems connecting to UTEP Information Resources, whether owned by the University or not, or whether standalone must install and enable current virus protection software.

The virus protection software must not be disabled or bypassed.

The settings for the virus protection software must not be altered in a manner that will reduce the effectiveness of the software.

The automatic update frequency of the virus protection software must not be altered to reduce the frequency of updates.

Any file server attached to UTEP Information Resources must utilize UTEP- approved virus protection software and must be setup to detect and clean viruses that may infect file shares.

Each E-mail gateway must utilize properly maintained email virus protection software this is UTEP–approved..

Any system identified as a security risk due to a lack of virus protection may be disconnected from the network or the respective network account may be disabled until adequate protection is in place.

Every know instance of a virus that is not automatically cleaned by the virus protection software constitutes a security incident and must be reported to the Information Security Office.

5.0 Disciplinary Actions

Violation of this policy may result in disciplinary action which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of UTEP Information Resources access privileges, civil, and criminal prosecution.

Revision History
First Draft: April 4, 2002
Revised: September 19, 2002
Revised: September 10, 2003
Revised: January 23, 2012

Wireless Communication

1.0 Introduction

In response to the increasing and widespread interest in wireless networking from individuals and departments, the University has developed wireless networking services that provide its users with the ability to move freely about the campus while utilizing the Internet.

Wireless networks pose significant challenges to stable and reliable operations of the campus network. The very flexibility and dynamism of wireless can inadvertently circumvent network topologies and security profiles in unpredictable ways, leading to failures and security exposure of critical infrastructure. Centrally designed and controlled wireless networks help to mitigate these exposures and reduce the time to troubleshoot problems when they occur.

Authentication for wireless networks is particularly important to enable notification of the owner of an improperly configured or malfunctioning device that interferes with normal network operations. Authentication also deters rogue activity and enables the University to assist law enforcement agencies as they investigate possible criminal activity. Absent authentication of wireless sessions, the networks in all buildings supporting unauthenticated connections are susceptible to failures unique to the local implementations, which could potentially affect critical infrastructure campus-wide.

Wireless networking, as implied by its name, has no dedicated medium–unlike wired systems. Signals used to convey data radiate across an uncontrolled spectrum at low power levels, competing with all other radiating sources (other computers, other wireless technologies, elevators, machinery, etc.). Isolating and troubleshooting problems or guaranteeing resources in such a dynamic environment is extremely difficult, and in some cases beyond current technical abilities. Necessarily, support for wireless systems is “best effort.” In contrast, wired systems provide a dedicated medium, the wire, and dedicated network equipment for the individual computers being connected, each of which can be easily isolated for troubleshooting, repair, and performance enhancements in a minimum amount of time. Consequently, activities requiring robust service levels should be supported on wired networks[1].

Individuals using a wireless network should proceed as if there were no guarantee of security on a wireless network. Therefore, it is recommended that information of a personal nature, information protected by FERPA or HIPAA regulations or PCI or any information the user would or should consider confidential not be transmitted over a wireless network.

2.0 Purpose

The purpose of the Wireless Communication Policy is to provide the best possible quality of wireless network service, ensure wired and wireless network security and integrity, and

[1] Portions of this section adapted from the “*Management of UTnet /Wireless Access Policy”, (http://www.utexas.edu/cio/policies/pdfs/Management%20of%20UTnet%20Wireless.pdf)*, with permission from ITS, The University of Texas at Austin, Austin, TX 78710-1110,

minimize interference between the campus wireless network and other products deployed throughout campus.

3.0 Scope

This policy covers all wireless data communication devices (e.g., personal computers, cellular phones, PDAs, tablets, etc.) connected to any of the University's Information Resources. This includes any form of wireless communication device capable of transmitting packet data. Wireless devices and/or networks without any connectivity to UTEP's Information Resources do not fall under the purview of this policy except that wireless access points or networks operating on campus without permission of the Telecommunications Infrastructure (TI) group or any device found to be interfering with the UTEP wireless networks are within the scope of this policy and subject to confiscation and removal from service.

4.0 Policy

Installation, engineering, maintenance, and operation of wired and wireless networks serving University faculty, staff, or students, on any property owned or tenanted by the University, are the sole responsibility of the Telecommunications Infrastructure group. Individuals and departments are prohibited from extending university networks through means wireless technologies.

5.0 Standards

For equipment supported by the UTEP please contact the TI group or the HelpDesk.

6.0 Enforcement

Violation of this policy may result in disciplinary action which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of UTEP Information Resources access privileges, civil, and criminal prosecution.

Revision History
First Draft: April 1, 2002
Revised: September 17, 2002
Revised: September 10, 2003
Revised: January 23, 2012

Web and Internet Access and Use

The University of Texas at El Paso (UTEP) 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 employees and students.

Because UTEP 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 Resources and there is no direct cost to the university attributable to such incidental use.

1.0 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 UTEP is easily identified as originating from the university network, some readers may assume that the university sponsors those publications. Even with disclaimers, the university is represented by its employees and staff and appropriate language, behavior and style is warranted.

2.0 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.
- The provision of operational instructions or information necessary to assist students, employees, and entities with which 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.
- 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.

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.

3.0 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.

4.0 Web Accounts

User accounts on the primary UTEP web server, 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, Academic Deans, or Academic Chairs).

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 to modify the password at the appropriate times.

5.0 Acceptable Use

- To facilitate communication and dissemination of information to UTEP faculty, staff, and students regarding university services and programs.
- To facilitate communication with current and prospective business partners for the daily operation of university business.
- To advertise and promote university programs and services to prospective students, professional colleagues, and the general population.
- To support professional societies, government advisory or standard activities related to the user's professional or vocational discipline.
- To apply for or administer grants or contracts for work-related applications.
- To announce products or services for use within the scope of university business, but not for commercial advertising of any kind.
- For official sites, any other communications or activities in direct support of university-related research, instruction, learning, dissemination of scholarly information, and administrative activities.
- 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.

6.0 Unacceptable Use

All Internet and web use is subject to the general policies governing use of the university's Information Resources. In addition, the following uses or contents are expressly forbidden on any university web page, official or individual:

- 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.
- Publishing or linking to legally restricted or confidential material.
- Publishing or linking to material that is obscene, libelous, physically threatening or otherwise in violation of standards for university publications.
- Publishing or linking to material that intentionally or negligently may lead to damage to a university or other computer system;
- 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.

7.0 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.

Revision History
First Draft: April 27, 2005
Revised: January 23, 2012

Definitions

ABUSE OF PRIVILEGE: When a user willfully performs an action prohibited by organizational policy or law, even if technical controls are insufficient to prevent the user from performing the action.

ACCEPTABLE RISK: A concern that has been determined to be a reasonable level of potential loss/disruption for a specific IT system due to the cost and magnitude of implementing countermeasures.

ACCESS: Opportunity to make use of an automated information system (AIS) resource.

ACCESS CONTROLS: Procedures and controls that limit or detect access to critical information resource assets (people, systems, applications, data, and/or facilities) to guard against loss of integrity, confidentiality, accountability, and/or availability.

ACCESS LEVEL: The hierarchical portion of the security level used to identify the sensitivity of data and the clearance or authorization of users. Note: The access level, in conjunction with the nonhierarchical categories, forms the sensitivity label of an object. See Security Level.

ACCESS LIST: A list of users, programs, and/or processes and the specifications of access categories to which each is assigned.

ACCESS MANAGEMENT: The planning, organization, direction, coordination, and evaluation of the system of accesses to data, which is initiated, transmitted, routed/gated, received, processed, and stored throughout a network.

ACCESS METHOD: (1) A software subsystem that provides input and output services as interface between an application and its associated devices. (2) A set of rules used by LAN hardware to direct traffic on the network.

ACCESS PASSWORD: A password used to authorize access to data and distributed to all those who are authorized similar access.

ACCESS PERIOD: A segment of time generally expressed on a daily or weekly basis, during which access rights prevail.

ACCESS PORT: A logical or physical identifier that a computer uses to distinguish different terminal input/output data streams.

ACCESS TYPE: The nature of an access right to a particular device, program, or file, e.g., read, write, execute, append, modify, delete, or create.

ACCOUNTABILITY: Principle that responsibilities for ownership and/or oversight of AIS resources are explicitly assigned and that assignees are answerable to proper authorities for stewardship of resources under their control.

ACCOUNTABILITY SERVICE NONREPUDIATION SERVICE: In cryptography, a service that prevents the originator from denying authorship at a later date.

ACCREDITATION: Authorization and approval granted to a major application or general support system to process in an operational environment. It is made on the basis of a certification by designated technical personnel that the system meets pre-specified technical requirements for achieving adequate system security. See Authorize Processing, Certification, Designated Approving Authority.

ACTIVE ATTACK: An attack that results in an unauthorized state change, such as the manipulation of files or the adding of unauthorized files.

ACTIVE HUB: A multi-ported device that amplifies LAN transmission signals.

ADD-ON SECURITY: The retrofitting of protection mechanisms implemented by hardware or software.

ADDRESS: A set of numbers, or data structure that uniquely identifies something, such as a network location or a particular process.

ADEQUATE SECURITY: Security commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information. This includes assuring that systems and applications operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost-effective management, acquisition, development, installation, operational, and technical controls.

ADMINISTRATIVE SECURITY: The management constraints and supplemental controls established to provide an acceptable level of protection for data. Synonymous with Procedural Security.

ADVANCED AUTHENTICATION SERVICES: Access management protocols (such as tokens or similar two factor authentication) employing single use, encrypted passwords for login procedures.

AES: Advanced Encryption Standard.

AGENCY: A department, commission, board, office, council, or other entity in the executive or judicial branch of government that is created by the constitution or a statute of this state, including a university system or institution of higher education.

AIS: See Automated Information System.

ALARM: A device used to alert a system administrator to suspicious activity or a security violation by a message, e-mail, or page.

ALE: See Annual Loss Expectancy.

ALERT: A formatted message describing a circumstance relevant to network security. Alerts are often derived from critical audit events.

ALGORITHMS: Complex mathematical formulae that are one component of encryption.

AMERICAN NATIONAL STANDARDS INSTITUTE (ANSI): The principal standards development body in the United States. ANSI is a nonprofit, nongovernmental body.

ANALOG: An electrical signal that varies continuously over an infinite range of voltage or electrical current values, as opposed to a digital signal, which varies discretely between two values, usually one and zero. It is the traditional method of voice transmission, whereas data is normally digital. In order to transmit digital signals across an analog network, it is first necessary to convert them into analog with a modem and reconvert them at the other end with another modem.

ANALYZE: To study or determine the nature and relationship of the parts.

ANKLE-BITER: A person who aspires to be a hacker/cracker but has very limited knowledge or skills related to AISs. Usually associated with young teens that collect and use simple malicious programs obtained from the Internet.

ANNUAL LOSS EXPECTANCY (ALE) = [Single loss expectancy] x [Rate of occurrence].

ANOMALY DETECTION MODEL: A model where intrusions are detected by looking for activity that is different from the user's or system's normal behavior.

ANSI: See American National Standards Institute.

API: See Application Programming Interface.

APPLICATION: A software program that carries out some useful task. Database managers, spreadsheets, communications packages, graphics programs, and work processors are all applications. Application software should be distinguished from system software, which is used by the computer itself to accomplish tasks for application software.

APPLICATION PROGRAMMING INTERFACE (API): A specification of function-call conventions that define an interface to a service or an application. They can be used to provide consistency across different types and brands of computers. Some APIs are adopted as de facto or de jure standards.

APPLICATION SYSTEM: A series of automated processes in full production and serving the needs of some part or all of an agency.

APPLICATION-BASED ATTACKS: Attacks that exploit vulnerabilities in applications by sending packets that communicate directly with an application.

APPLICATION-LEVEL FIREWALL: A firewall system in which service is provided by processes that maintain a connection state and sequencing while forwarding and filtering

message traffic between external and internal hosts. Application-level firewalls (ALFs) often re-address traffic (a.k.a. network address translation) so that outgoing traffic appears to have originated from a range of addresses assigned to the firewall, rather than the address of the internal host. ALFs often provide remote access services (such as dial in/out), real time (or near real time) alerts and comprehensive logging of message traffic. See Firewall, Packet Filtering, Proxy.

APPLICATION-LEVEL GATEWAY (FIREWALL): A firewall system in which service is provided by processes that maintain complete TCP connection state and sequencing. Application-level firewalls often re-address traffic so that outgoing traffic appears to have originated from the firewall, rather than the internal host.

ARA: AVERT Risk Assessment. The first early warning system created by virus research experts with the goal of helping network administrators assess the risk associated with new virus outbreaks.

ARCHITECTURE: The manner in which hardware or software is structured. Architecture typically describes how the system or program is constructed, how its components fit together, and the protocols and interfaces used for communication and cooperation among modules or components of the system. Network architecture defines the functions and description of data formats and procedures used for communication between nodes or workstations.

ASIM: See Automated Security Incident Measurement.

ASSESS: To evaluate the extent to which certain factors (threats, vulnerabilities, and risks) affect the IT environment.

ASSESSMENT SURVEYS AND INSPECTIONS: An analysis of the vulnerabilities of an AIS. Information acquisition and review process designed to assist a customer to determine how best to use resources to protect information in systems.

ASSET: Any information resource with value that is worth protecting or preserving.

ASSURANCE: A measure of confidence that the security features and architecture of an AIS accurately mediate and enforce the security policy.

ASYMMETRIC CRYPTOSYSTEM: A method of encryption in which two different keys are used: one for encrypting and one for decrypting the data (e.g., public-key encryption).

ASYMMETRIC KEY CRYPTOGRAPHY: Based on a mathematical discovery in the 1970s, there exist pairs of numbers such that data encrypted with one member of the pair can be decrypted by the other member of the pair and by no other means. The number made known to the public is called the public key; the number kept secret is called the private key. Also called Public Key Cryptography.

ASYNCHRONOUS: A method of transmitting data one bit at a time. It is the simplest form of communication. It is a low-cost alternative to synchronous communications.

ATM: Asynchronous Transfer Mode.

ATTACK: An attempt to bypass the physical or information security measures and controls protecting an AIS. The attack may alter, release, or deny data. Whether an attack will succeed depends on the vulnerability of the computer system and the effectiveness of existing countermeasures. See Penetration, Intrusion.

ATTACK SIGNATURE: Activities or alterations to an AIS indicating an attack or attempted attack, detectable by examination of audit trail logs.

ATTACKER: A person accessing workstation, system, or networked resources without valid authorization.

AUDIT: The independent examination of records and activities to ensure compliance with established controls, policy, and operational procedures, and to recommend any indicated changes in controls, policy, or procedures.

AUDIT TRAIL: A chronological record of system activities that is sufficient to enable the reconstruction, review, and examination of the sequence of environments and activities surrounding or leading to an operation, a procedure, or an event in a transaction from its inception to final results. This includes user login, file access, other various activities, and whether any actual or attempted security violations occurred, legitimate and unauthorized.

AUDIT/ARCHIVE TOOLS: Hardware, software, and network tools that organize and provide for the storage and protection of information gathered by the sensors.

AUTHENTICATE: To establish the validity of a claimed user or object.

AUTHENTICATION: The process of confirming a claimed identity. All forms of authentication are based on something you know, something you have, or something you are.

- 'Something you know' is some form of information that you can recognize and keep to yourself, such as a personal identification number (PIN) or password.
- 'Something you have' is a physical item you possess, such as a photo ID or a security token.
- 'Something you are' is a human characteristic considered to be unique, such as a fingerprint, voice tone, or retinal pattern.

AUTHENTICATION HEADER (AH): A field that immediately follows the IP header in an IP datagram and provides authentication and integrity checking for the datagram.

AUTHENTICATION TOKEN: A portable device used for authenticating a user. Authentication tokens operate by challenge/response, time-based code sequences, event synchronous or other techniques. This may include paper-based lists of one-time passwords.

AUTHORITY: An entity recognized by a set of secure systems as a trusted source of security information. An authority may be online, as an authentication service, or offline, as a certification authority.

AUTHORIZATION: The act of granting permission for someone or something to conduct an act. Even when identity and authentication have indicated who someone is, authorization may be needed to establish what actions are permitted.

AUTHORIZE PROCESSING: Occurs when management authorizes a system based on an assessment of management, operational and technical controls. By authorizing processing in a system the management official accepts the risk associated with it. See Accreditation, Certification, Designated Approving Authority.

AUTOMATED INFORMATION SYSTEM (AIS): An assembly of computer hardware, firmware, and software configured to collect, create, communicate, compute, disseminate, process, store, and/or control data or information.

AUTOMATED SECURITY INCIDENT MEASUREMENT: Monitors network traffic and collects information on targeted unit networks by detecting unauthorized network activity.

AUTOMATED SECURITY MONITORING: All security features needed to provide an acceptable level of protection for hardware, software, and classified, confidential, unclassified or critical data, material, or processes in the system.

AUTOMATIC KEY UPDATES: The transparent renewal of certificates and key pairs.

AVAILABILITY: Availability represents the requirement that an asset or resource be accessible to authorized person, entity, or device. **AVAILABILITY PROTECTION:** Requires backup of system and information, contingency plans, disaster recovery plans, and redundancy. Examples of systems and information requiring availability protection are time-share systems, mission-critical applications, time and attendance, financial, procurement, or life-critical.

AVERT: Anti-Virus Emergency Response Team.

AWARENESS: A learning process that sets the stage for training by changing individual and organizational attitudes to realize the importance of security and the adverse consequences of its failure.

AWARENESS, TRAINING AND EDUCATION: Includes: (1) awareness programs set the stage for training by changing organizational attitudes toward realization of the importance of security and the adverse consequences of its failure; (2) the purpose of training is to teach people the skills that will enable them to perform their jobs more effectively; (3) education is more in-depth than training and is targeted for security professionals and those whose jobs require expertise in automated information security.

BACK DOOR: A feature built into a program by its designer, which allows the designer special privileges that are denied to the normal users of the program. A back door in an EXE or COM program, for instance, could enable the designer to access special set-up functions.

BACKBONE NETWORK: A network acting as a primary conduit for traffic that is often both sourced from, and destined for, other networks.

BACKGROUND SCANNING: Automatic scanning of files as they are created, opened, closed, or executed. Performed by memory resident anti-virus software.

BACKUP: Copy of files and applications made to avoid loss of data and facilitate recovery in the event of a system crash.

BANDWIDTH: A measure of the transmission capacity of a communications channel. Digital transmission is expressed in bits or bytes per second. Analog transmission is measured in cycles per second (Hertz - Hz). Bandwidth varies with the type and method of transmission. The more bandwidth a network has, the more information it can carry.

BANNER: Display on an AIS that sets forth conditions and restrictions on system and/or data use.

BASELINE SECURITY: The minimum-security controls required for safeguarding an IT system based on its identified needs for confidentiality, integrity, and/or availability protection.

BASTION HOST: A system that has been hardened to resist attack, and which is installed on a network in such a way that it is expected to potentially come under attack. Bastion hosts are often components of firewalls, or may be "outside" Web servers or public access systems. Generally, a bastion host is running some form of general-purpose operating system (e.g., UNIX, VMS, NT, etc.) rather than a ROM-based or firmware operating system (e.g., IOS). See Firewall.

BATCH PROCESSING: A type of data processing where related transactions are grouped, transmitted, and processed together by the same computer at the same time. A type of processing where time is not critical and no user input is needed while the processing takes place. The other type of data processing is called "real time."

BEHAVIOR BLOCKING: A set of procedures that are tuned to detect virus-like behavior, and prevent that behavior (and/or warn the user about it) when it occurs. Some behaviors that should normally be blocked in a machine include formatting tracks, writing to the master boot record, and writing directly to sectors.

BEHAVIORAL OUTCOME: What an individual who has completed the specific training module is expected to be able to accomplish in terms of IT security-related job performance.

BELL-LA PADULA SECURITY MODEL: Formal state-transition model of computer security policy that describes a formal set of access controls based on information sensitivity and subject authorizations.

BIBA INTEGRITY MODEL: A formal security model for the integrity of subjects and objects in a system.

BIMODAL VIRUS: A virus that infects both boot records and files. Also called bipartite or multipartite. See File Virus, Boot Sector-Infecting Virus.

BIOMETRICS: Automated methods of authenticating or verifying a user based on physical or behavioral characteristics.

BIT: A binary unit of information that can have either of two values, 0 or 1. The most basic way of storing and transmitting information. Contraction of Binary digit.

BOMB: A general synonym for crash, normally of software or operating system failures.

BOOT: To start a computer so that it is ready to run programs for the user.

BOOT RECORD: The program recorded in the Boot Sector. All floppies have a boot record, whether or not the disk is actually bootable. Whenever you start or reset your computer with a disk in the A: drive, DOS reads the boot record from that diskette. If a boot virus has infected the floppy, the computer first reads the virus code in (because the boot virus placed its code in the boot sector), then jumps to whatever sector the virus tells the drive to read, where the virus has stored the original boot record.

BOOT RECORDS: Those areas on diskettes or hard disks that contain some of the first instructions executed by a PC when it is booting. Boot records must be loaded and executed in order to load the operating system. Viruses that infect boot records change the boot records to include a copy of themselves. When the PC boots, the virus program is run and will typically install itself in memory before the operating system is loaded.

BOOT SECTOR: The first logical sector of a drive. On a floppy disk, this is located on side 0 (the top), cylinder 0 (the outside), sector 1 (the first sector). On a hard disk, it is the first sector of a logical drive, such as C: or D:. This sector contains the Boot Record, which is created by FORMAT (with or without the /S switch.) The sector can also be created by the DOS SYS command. Any drive that has been formatted contains a boot sector.

BOOT SECTOR INFECTOR: Every logical drive, both hard disk and floppy, contains a boot sector. This is true even of disks that are not bootable. This boot sector contains specific information relating to the formatting of the disk, the data stored there and also contains a small program called the boot program (which loads the DOS system files). The boot program displays the familiar "Non-system Disk or Disk Error" message if the DOS system files are not present. It is also the program that gets infected by viruses. You get a boot sector virus by leaving an infected diskette in a drive and rebooting the machine. When the program in the boot sector is read and executed, the virus goes into memory and infects your hard drive. Remember, because every disk has a boot sector, it is possible (and common) to infect a machine from a data disk.

BOOT SECTOR-INFECTING VIRUS: Some viruses infect the boot records of hard disks and diskettes. They typically do so by replacing the existing boot record with their own code. The virus is executed when the system is booted from the hard disk or diskette, and installs its own code in the system's memory so that it can infect other hard disks or diskettes later. Once that has happened, the virus will usually execute the normal boot program, which it stores elsewhere on the disk

BOOT VIRUS: A virus whose code is called during the phase of booting the computer in which the master boot sector and boot sector code is read and executed. Such viruses either place their starting code or a jump to their code in the boot sector of floppies, and either the boot sector or master boot sector of hard disks. Most boot viruses infect by moving the original code of the master boot sector or boot sector to another location, such as slack space, and then placing their own code in the master boot sector or boot sector. Boot viruses also infect files are sometimes known as multipartite viruses. All boot viruses infect the boot sector of floppy disks; some of them, such as Form, also infect the boot sector of hard disks. Other boot viruses infect the master boot sector of hard disks.

BREACH: The successful defeat of security controls that could result in a penetration of the system. A violation of controls of a particular information system such that information assets or system components are unduly exposed.

BRIDGE: (1) A device that connects two networks of the same type together. (2) A device that connects and passes packets between two network segments having the same data-link frame type. Bridges operate at Layer 2 of the OSI reference model (data-link layer) and are insensitive to upper-layer protocols. See Router.

BROWSER: An application with a graphical user interface (GUI) that allows a user to access information on the World Wide Web.

BROWSING: The act of searching through storage to locate or acquire information without necessarily knowing of the existence or the format of the information being sought.

BUFFER OVERFLOW: This happens when more data is put into a buffer or holding area than the buffer can handle. This is due to a mismatch in processing rates between the producing and consuming processes. This can result in system crashes or the creation of a back door leading to system access.

BUG: An error in the design or implementation of a program that causes it to do something that neither the user nor the program author had intended.

BUSINESS CONTINUITY PLAN (BCP): The documentation of a predetermined set of instructions or procedures that describe how an organization's business functions will be sustained during and after a significant disruption.

BUSINESS IMPACT ANALYSIS (BIA): An analysis of an IT system's requirements, processes, and interdependencies used to characterize system contingency requirements and priorities in the event of a significant disruption

BYTE: A group of eight bits. Often used to represent a character. Bytes are also units of storage and transmission.

C2: Command and Control.

C2-ATTACK: Prevent effective C2 of adversary forces by denying information to or by influencing, degrading, or destroying the adversary C2 system.

C2-PROTECT: Maintain effective command and control of own forces by turning to friendly advantage or negating adversary effort to deny information to or to influence, degrade, or destroy the friendly C2 system.

C2W: See Command and Control Warfare.

CA: See Certification Authority.

CABLE MODEM: Cable companies such as AT&T Broadband provide Internet access over Cable TV coaxial cable. A cable modem accepts this coaxial cable and can receive data from the Internet at over 1.5 Mbps. Cable is currently available only in certain communities.

CABLING: The medium that connects nodes on a network. Cabling can be twisted-pair, coaxial, or fiber optic.

CALL BACK: A procedure for identifying a remote terminal. In a call back, the host system disconnects the caller and then dials the authorized telephone number of the remote terminal to reestablish the connection. Synonymous with Dial Back.

CARRIER: Alternating current that vibrates at a fixed frequency and is used to establish an envelope in which a signal is transmitted. Also refers to long-distance companies such as MCI, Sprint, or AT&T.

CATASTROPHIC DISASTER: A disaster in which the damage sustained is sufficiently severe as to render the data processing activity incapable of providing support to the agency; and the condition is anticipated to last for an indefinite period of time.

CATEGORY I DATA: Are university data protected specifically by federal or state law or University of Texas rules and regulations (e.g., HIPAA; FERPA; Sarbanes-Oxley, Gramm-Leach-Bliley; the Texas Identity Theft Enforcement and Protection Act; University of Texas System Business Procedure Memoranda; specific donor or employee data). University data that are not otherwise protected by a known civil statute or regulation, but which must be protected due to university contractual agreements requiring confidentiality, integrity, or availability considerations (e.g., Non Disclosure Agreements, Memoranda of Understanding, Service Level Agreements, Granting or Funding Agency Agreements, etc.) are also included.

CATEGORY II DATA: Are university data not otherwise identified as Category-I data, but which are releasable in accordance with the Texas Public Information Act (e.g., contents of specific e-mail, date of birth, salary, etc.) Such data must be appropriately protected to ensure a controlled and lawful release.

CATEGORY III DATA: Are university data that are not otherwise identified as Category-I or Category-II data (e.g., publicly available). Such data have no requirement for confidentiality, integrity, or availability.

CCITT: Consultative Committee for International Telegraph and Telephone. An international organization that develops communications standards. They have recently been renamed to the International Telecommunications Union (ITU).

CERT: See Computer Emergency Response Team.

CERTIFICATE: Digital record holding security information about a user (generally, the user's public key for data encryption).

CERTIFICATION: Synonymous with Authorize Processing. Certification is the technical evaluation that establishes the extent to which a computer system, application, or network design and implementation meets a pre-specified set of security requirements. See Accreditation, Authorize Processing.

CERTIFICATION AUTHORITY (CA): A trusted third party whose purpose is to sign certificates for network entities it has authenticated using secure means. Other network entities can check the signature to verify that a CA has authenticated the bearer of a certificate. **CGI:** Common Gateway Interface. CGI is the method that Web servers use to allow interaction between servers and programs.

CGI SCRIPTS: Allows for the creation of dynamic and interactive Web pages. CGI scripts also tend to be the most vulnerable part of a Web server (besides the underlying host security).

CHALLENGE/RESPONSE: An authentication technique whereby a server sends an unpredictable challenge to the user, who computes a response using some form of authentication token.

CHANGE: Any implementation of new functionality; any interruption of service; any repair of existing functionality; any removal of existing functionality.

CHANGE CONTROL: See Configuration Management.

CHANGE MANAGEMENT: The process of controlling modifications to hardware, software, firmware, and documentation to ensure that Information Resources are protected against improper modification before, during, and after system implementation.

CHANNEL: Any pathway between two computers or between a terminal and a computer. It may be physical, such as twisted-pair wiring, coaxial cable, or optical fibers; or it may be a specific carrier frequency within a larger channel.

CHANNEL BANK: A device used to each end of time-division-multiplex transmission systems to divide the bandwidth into separate channels and to provide control of those channels.

CHANNEL SERVICE UNIT (CSU): A digital interface device that connects end-user equipment to the local digital telephone loop.

CHAP: Challenge Handshake Authentication Protocol is an authentication method that uses a one-way hashing function. DLCI Data Link Connection Identifier (DLCI) is a unique number assigned to a Permanent Virtual Circuit (PVC) end point in a frame relay network. DLCI

identifies a particular PVC endpoint within a user's access channel in a frame relay network, and has local significance only to that channel.

CHECK_PASSWORD: A hacking program used for cracking VMS passwords.

CHECKSUM: A value automatically computed on data to detect error or manipulation during transmission.

CHERNOBYL PACKET: Also called Kamikaze Packet. A network packet that induces a broadcast storm and network meltdown. Typically an IP Ethernet datagram that passes through a gateway with both source and destination Ethernet and IP address set as the respective broadcast addresses for the sub networks being gated between.

CHIEF INFORMATION SECURITY OFFICER (CISO): The individual responsible for this function shall report to the IRM and is responsible for directing policies and procedures designed to protect Information Resources. This function includes Monitors University Information Resources; Identifies vulnerabilities; Identifies critical and confidential Information Resources; Develops/Maintains a Risk Management Program; and Develops/Maintains an adequate Security Program.

CIPHER: An algorithm for encryption and decryption in which arbitrary symbols or groups of symbols are used to represent plain text, or in which units of plain text are rearranged, or both.

CIPHER TEXT: Encrypted data.

CIRCUIT: A communications channel. Technically, any path that can carry electrical current.

CIRCUIT-LEVEL GATEWAY: One form of a firewall. Validates TCP and UDP sessions before opening a connection. Creates a handshake, and once that takes place passes everything through until the session is ended.

CISO: See Chief Information Security Officer

CLASSIFIED INFORMATION: Information that has been determined under an applicable authority to require protection against unauthorized disclosure.

CLIENT/SERVER ARCHITECTURE: An architecture consisting of server programs that await and fulfill requests from client programs on the same or another computer.

CLIENT/SERVER COMPUTING: Term used to describe distributed processing (computing) network systems in which transaction responsibilities are divided into two parts: client and server. A client is a requester of a service; a server is a provider of a service.

CLIPPER CHIP: A tamper-resistant VLSI chip designed by NSA for encrypting voice communications. It conforms to the Escrow Encryption Standard (EES) and implements the Skipjack encryption algorithm.

CLOSED SECURITY ENVIRONMENT: An environment that includes those systems in which both of the following conditions hold true. (1) Application developers (including maintainers) have sufficient clearances and authorizations to provide an acceptable presumption that they have not introduced malicious logic. Sufficient clearance is defined as follows: where the maximum classification of data to be processed is confidential or below, developers are cleared and authorized to the same level as the most sensitive data; where the maximum classification of data to be processed is secret or above, developers have at least a secret clearance. (2) Configuration control provides sufficient assurance that applications are protected against the introduction of malicious logic prior to and during operation of system applications.

CLUSTER VIRUS: A virus that infects disks or diskettes by modifying their file systems so that every program file entry points to the virus code. The virus code only exists in one physical place on the disk, but running any program on the disk will run the virus as well. Thus, cluster viruses can appear to infect every program on a disk.

CNA: See Computer Network Attack.

COAST: Computer Operations, Audit, and Security Technology is a multiple project, multiple investigator laboratory in computer security research in the Computer Sciences Department at Purdue University. It functions with close ties to researchers and engineers in major companies and government agencies. Its research is focused on real-world needs and limitations, with a special focus on security for legacy computing systems.

CODE: In computer programming, a set of symbols used to represent characters and format commands and instructions in a program.

COLD SITE: An alternate site with necessary electrical and communications connections and computer equipment, but no running system, maintained by an organization to facilitate prompt resumption of service after a disaster. See Hot Site.

COM FILE: A PC-DOS binary image that is loaded into memory. It has restrictions in size and method of program load. It generally loads somewhat faster than an EXE file and has a simpler structure.

COMMAND AND CONTROL WARFARE (C2W): The integrated use of operations security, military deception, psychological operations, electronic warfare, and physical destruction, mutually supported by intelligence, to deny information to or to influence, degrade, or destroy adversary command and control capabilities, while protecting friendly command and control capabilities against such actions. Command and control warfare is an application of information operations in military operations and is a subset of information warfare. C2W is both offensive and defensive.

COMMAND CENTER: A temporary location with communication equipment from which initial recovery efforts are manned and media-business communication is maintained.

COMMERCIAL OFF-THE-SHELF SOFTWARE (COTS): This software is a standard, commercial product, not developed by a vendor for a particular project.

COMMON CRITERIA: The international harmonization of existing computer security criteria that is planned to replace the TCSEC as the U.S. national criteria.

COMMON SECURITY MODEL: A mathematical description of subjects, objects, and other entities of a system for the purpose of analyzing the security of the system.

COMMUNICATIONS SECURITY (COMSEC): The protection that insures the authenticity of telecommunications and results from the application of measures taken to deny unauthorized persons information of value which might be derived from the acquisition of telecommunications.

COMPANION VIRUS: A virus that creates a new program with the same file name as an existing program, but in a different place or with a different file type, so that typing the program's name on the command line causes the virus program to be executed instead of the original program. For instance, a companion virus could create a file name FOO.COM that contained its code, if a program named FOO.EXE already existed. When the user types FOO on the command line, FOO.COM would get executed instead of FOO.EXE.

COMPARTMENTED MODE: An AIS is operating in compartmented mode when each user with direct or indirect access to the AIS, its peripherals, remote terminals, or remote hosts, has all of the following:(1) a valid personnel clearance for the most restricted information processed in the AIS; (2) formal access approval for, and has signed nondisclosure agreements for, that information to which he/she is to have access; (3) a valid need-to-know for that information to which he/she is to have access.

COMPROMISE: A breach of security policy involving unauthorized disclosure, modification, destruction, or loss of information, whether deliberate or unintentional.

COMPROMISING EMANATIONS: Unintentional data related or intelligence-bearing signals that, if intercepted and analyzed, disclose the classified information transmission received, handled, or otherwise processed by any information processing equipment.

COMPUTER: A machine that can be programmed in code to execute a set of instructions (program). In an AIS, the term computer usually refers to the components inside the case: the motherboard, memory chips, and internal storage disk(s).

COMPUTER ABUSE: The willful or negligent unauthorized activity that affects the availability, confidentiality, or integrity of computer resources. Computer abuse includes fraud, embezzlement, theft, malicious damage, unauthorized use, denial of service, and misappropriation. See Computer Fraud.

COMPUTER INCIDENT RESPONSE TEAM (CIRT): Personnel responsible for coordinating the response to computer security incidents in an organization.

COMPUTER FRAUD: Computer-related crimes involving deliberate misrepresentation, alteration or disclosure of data in order to obtain something of value (usually for monetary gain). A computer system must have been involved in the perpetration or cover-up of the act or series of acts. A computer system might have been involved through improper

manipulation of input data, output or results, applications programs, data files, computer operations, communications, or computer hardware, systems software, or firmware.

COMPUTER LANGUAGE: A language used to generate programs.

COMPUTER NETWORK: A set of computers that is connected and able to exchange data.

COMPUTER NETWORK ATTACK (CNA): Operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.

COMPUTER ORACLE AND PASSWORD SYSTEM (COPS): A computer network monitoring system for UNIX machines. Software tool for checking security on shell scripts and C programs. Checks for security weaknesses and provides warnings.

COMPUTER SECURITY: Measures and controls that ensure confidentiality, integrity, and availability of AIS assets, including hardware, software, firmware, and information being processed, stored, and communicated. Synonymous with Information Systems Security.

COMPUTER SECURITY INCIDENT: Any intrusion or attempted intrusion into an AIS. Incidents can include probes of multiple computer systems.

COMPUTER SECURITY INCIDENT RESPONSE CAPABILITY (CSIRC): A set of policies and procedures defining security incidents and governing the actions to be taken when they occur.

COMPUTER SECURITY INTRUSION: Any event of unauthorized access or penetration to an AIS.

COMPUTER SECURITY PROGRAM: Synonymous with IT Security Program.

COMSEC: See Communications Security.

CONCEPT OF OPERATIONS (CONOP): Document detailing the method, act, process, or effect of using an AIS.

CONFIDENTIAL: The classification of data of which unauthorized disclosure/use could cause serious damage to an organization.

CONFIDENTIAL INFORMATION: Information maintained by state agencies that is exempt from disclosure under the provisions of the Public Records Act or other applicable state or federal laws. The controlling factor for confidential information is dissemination.

CONFIDENTIALITY: Assurance that information is not disclosed to unauthorized persons, processes, or devices.

CONFIDENTIALITY PROTECTION: Requires access controls such as user ID/passwords, terminal identifiers, and restrictions on actions like read, write, delete, etc. Examples of confidentiality-protected information are personnel, financial, proprietary

CONFIGURATION: The physical format or design of a communications network. The physical topology of a communications network which includes end nodes, transmission nodes, and interconnecting data transmission lines.

CONFIGURATION CONTROL: Process of controlling modifications to hardware, software, firmware, and documentation to ensure that an AIS is protected against improper modification before, during, and after system implementation.

CONFIGURATION MANAGEMENT: Management of security features and assurances through control of changes made to hardware, software, firmware, documentation, test, test fixtures, and test documentation throughout the life cycle of an AIS.

CONOP: Concept of operations.

CONSEQUENCE: Outcome, effect.

CONSULTATIVE COMMITTEE FOR INTERNATIONAL TELEGRAPH AND TELEPHONE (CCITT): An international organization that develops communications standards. They have recently been renamed to the International Telecommunications Union (ITU).

CONTINGENCY PLAN: A plan maintained for emergency response, backup operations, and post-disaster recovery for an AIS, to ensure availability of critical resources and to facilitate the continuity of operations in an emergency.

CONTROL: A protective action, device, procedure, technique, or other measure that reduces exposure.

CONTROLLED MODE: The mode of operation that is a type of multilevel security mode in which a more limited amount of trust is placed in the hardware/software base of the system, with resultant restrictions on the classification levels and clearance levels that may be supported.

CONTROLS: A configuration, design, method, procedure, or process, which implements organizational policy. Technical controls are built into information systems to provide some form of automated enforcement of policy. See Policy.

COPS: See Computer Oracle and Password System.

COTS: See Commercial Off-the-Shelf Software.

COUNTERMEASURES: Any action, device, procedure, technique, or other measure that mitigates risk by reducing the vulnerability of, threat to, or impact on a system.

COUPLING: Interaction between systems or between properties of a system.

COVERT CHANNEL: A communications channel that allows a process to transfer information in a manner that violates the system's security policy.

COVERT TIMING CHANNEL: A covert channel in which one process signals information

CPU: Abbreviation for central processing unit.

CRACK: A popular hacking tool used to decode encrypted passwords. System administrators also use Crack to assess weak passwords by novice users in order to enhance the security of the AIS.

CRACKER: One who breaks security on an AIS.

CRACKING: The act of breaking into a computer system.

CRASH: A sudden, usually drastic failure of a computer system.

CRC: See Cyclic Redundancy Code.

CREDENTIALS: Something you know (e.g., a password or pass phrase), and/or something that identifies you (e.g., a user name, a fingerprint, voiceprint, retina print). Something you know and something that identifies you are presented for authentication.

CRITICAL: Crucial, decisive.

CRITICAL APPLICATION: The prioritization of application systems that are classified by the agency as being essential in performing the agency mission.

CRITICAL ASSET: An asset that is essential to the agency's mission critical functions and/or impacts public health, public safety, and revenue collection and distribution.

CRITICAL INFORMATION RESOURCE: That resource determined by agency management to be essential to the agency's critical mission and functions, the loss of which would have an unacceptable impact.

CRITICAL INFRASTRUCTURE: Physical or cyber-based system essential to the minimum operations of the economy and government.

CROSS CERTIFICATION: A means for two certifications authorities to trust each other.

CRYPTANALYSIS: (1) The analysis of a cryptographic system and/or its inputs and outputs to derive confidential variables and/or sensitive data including clear text. (2) Definition: operations performed in converting encrypted messages to plain text without initial knowledge of the crypto-algorithm and/or key employed in the encryption.

CRYPTOGRAPHIC HASH FUNCTION: A process that computes a value (referred to as a hash word) from a particular data unit in a manner that, when a hash word is protected, manipulation of the data is detectable.

CRYPTOGRAPHY: The science of transforming data so that it is interpretable only by authorized persons.

CRYPTOLOGY: The science that deals with hidden, disguised, or encrypted communications.

CSIRC: See Computer Security Incident Response.

CSU: See Channel Service Unit.

CUSTODIAN: Guardian or caretaker; the holder of data, the agent charged with implementing the controls specified by the owner. The custodian is responsible for the processing and storage of information. The custodians of information resources, including entities providing outsourced information resources services to the university, must:

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

CYBERSPACE: Describes the world of connected computers and the society that gathers around them. Commonly known as the Internet.

CYCLIC REDUNDANCY CODE: A CRC is a type of checksum. A checksum algorithm takes a file (or other string of bytes) and calculates from it a few bytes (the checksum) that depend on the entire file. The idea is that if anything in the file changes, the checksum will change. CRC checksums are usually used to detect random, uncorrelated changes in files.

DAA: See Designated Approving Authority.

DARK-SIDE HACKER: A criminal or malicious hacker.

DARPA: Department of Defense Advanced Research Projects Agency. This agency sponsored the network architecture research project upon which ARPANET is based, now known as the Internet.

DATA: A representation of facts or concepts in an organized manner in order that it may be stored, communicated, interpreted, or processed by automated means.

DATA ARCHITECTURE: The overall structure of the data of the enterprise. It includes the definition of subject databases, distribution architecture, and a definition of the major data policy decisions as well as the logical and physical definitions of the data-structures of the enterprise.

DATA DRIVEN ATTACK: A form of attack that is encoded in innocuous seeming data that is executed by a user or a process to implement an attack. A data driven attack is a concern for firewalls, since it may get through the firewall in data form and launch an attack against a system behind the firewall.

DATA ENCRYPTION STANDARD (DES): An encryption algorithm that has been endorsed by both the U.S. National Institute for Standards and Technology (NIST) and the American National Standards Institute (ANSI) as providing adequate security for unclassified information.

DATA INTEGRITY: A condition existing when data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed.

DATA LINK LAYER: The second layer of the OSI data communications model. It is the level that puts messages together and coordinates their flow such that the channel appears to be free of transmission errors to the network layer.

DATA OWNER: The authority, individual, or organization that has original responsibility for the data by statute, executive order, or directive.

DATA RISK: The risks involving integrity, disclosure, and recovery issues.

DATA SECURITY OR COMPUTER SECURITY: Those measures, procedures, or controls that provide an acceptable degree of safety of information resources from accidental or intentional disclosure, modification, or destruction.

DATA STEWARD: University representatives, such as faculty, staff, or researchers, who are tasked with managing administrative and/or research data owned by the university. Such data is to be managed by a data steward as a university resource and asset. The data steward has the responsibility of ensuring that the appropriate steps are taken to protect the data and that respective policies and guidelines are being properly implemented. Data Stewards may delegate the implementation of university policies and guidelines to professionally trained campus or departmental IT custodians.

DATABASE: A collection of interrelated data stored together in electronic form, with controlled redundancy, to serve one or more applications. The data is stored so that it is independent from programs that use the data; a common and controlled approach is used in adding new data and in modifying and retrieving existing data within a database. A database may be distributed.

DCE: See Distributed Computing Environment.

DE FACTO STANDARD: A programming language, product, design, or program that has become so widely used and imitated that it has little competition, but those whose status has not officially been declared by a recognized standard establishing organization.

DE JURE STANDARD: A standard that exists in the market place due to their adoption by standard approving bodies, such as ANSI and ISO.

DECLASSIFICATION: An administrative decision or procedure to remove or reduce the security classification of the subject media.

DEDICATED CHANNEL: A communications line or circuit that is not switched and is used exclusively for one purpose or to connect to specific locations or machines. When the line is not customer-owned, the term leased line is more common.

DEDICATED SECURITY MODE: A mode of operation wherein all users have the clearance, authorization, or documented formal access approval, if required, and the need-to-know for all data handled by the AIS. If the AIS processes special access information, all users require formal access approval. In the dedicated mode, an AIS may handle a single classification level and/or category of information or a range of classification levels and/or categories.

DEFENSIVE INFORMATION OPERATIONS: A process that integrates and coordinates policies and procedures, operations, personnel, and technology to protect information and defend information systems. Defensive information operations are conducted through information assurance, physical security, operations security, counter deception, counter-psychological operations, counter-intelligence, electronic protect, and special information operations. Defensive information operations ensure timely, accurate, and relevant information access while denying adversaries the opportunity to exploit friendly information and information systems for their own purposes.

DEGAUSS: To apply a variable, alternating current (AC) field for the purpose of demagnetizing magnetic recording media, usually tapes. The process involves increasing the AC field gradually from zero to some maximum value and back to zero, which leaves a very low residue of magnetic induction on the media.

DEMON DIALER: A program that repeatedly calls the same telephone number. This is benign and legitimate for access to a bulletin board system or malicious when used as a denial of service attack.

DENIAL OF SERVICE: Result of any action or series of actions that prevent any part of an AIS from providing data or other services to authorized users.

DENIAL OF SERVICE ATTACK (DoS): An attack on a network that is designed to bring the network to its knees by flooding it with useless traffic. Many DoS attacks, such as the Ping of Death and Teardrop attacks, exploit limitation in the TCP/IP protocols. For all known DoS attacks, there are software fixes that system administrators can install to limit the damage caused by the attacks. But, like viruses, new DoS attacks are constantly being dreamed up by hackers.

DERF: The act of exploiting a terminal that someone else has absent-mindedly left logged on.

DES: See Data Encryption Standard.

DESIGNATED APPROVING AUTHORITY (DAA): The official who has the authority to decide on accepting the security safeguards prescribed for an AIS or the official who may be responsible for issuing an accreditation statement that records the decision to accept those safeguards. The DAA must be at an organizational level such that he or she has authority to

evaluate the overall mission requirements of the AIS and to provide definitive directions to AIS developers or owners relative to the risk in the security posture of the AIS.

DEVICE: An entity that can access a network. Used interchangeably with node.

DIAL BACK: Synonymous with Call Back.

DIAL-IN MODEM: A peripheral device that connects computers to each other for sending communications via the telephone lines. The modem modulates the digital data of computers into analog signals to send over the telephone lines, then demodulates back into digital signals to be read by the computer on the other end; thus the name "modem" for modulator/demodulator.

DIAL-UP: **This service is not longer supported as of September 1, 2011**. The service whereby a computer terminal can use the telephone to initiate and effect communication with a computer.

DIAL-UP LINE: **This service is no longer supported as of September 1, 2011**. Communications circuit that is established by a switched-circuit connection using the telephone network.

DICTIONARY ATTACK: An attempt to gain access to an AIS by guessing a user's password, using software that systematically enters words in a dictionary as passwords until a match is found. See Password Cracker.

DIGITAL RESEARCH DATA: Are defined as the subset of research data as defined below that are transmitted by or maintained in, electronic format and include any of the following: (a) Electronic storage data including storage devices in computers (hard drives, memory) and any removable/transportable digital storage medium, such as magnetic tape or disk, optical disk, or digital memory card; or (b) Transmission data used to exchange information already in electronic storage format. Transmission data include, for example, the Internet (wide-open), extranet (using Internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, private networks, intranet, and the physical movement of removable/transportable electronic storage data.

DIGITAL SIGNATURE: Cryptographic process used to assure the authenticity and nonrepudiation of a message originator and/or the integrity of a message.

DIGITAL SIGNATURE SERVICE: In cryptography a service that guarantees the identity of the originator of the message

DIRECTORY: Somewhere to store certificates and certificate revocation list (CRL).

DISASTER: A condition in which an information resource is unavailable, as a result of a natural or man-made occurrence, that is of sufficient duration to cause significant disruption in the accomplishment of agency program objectives, as determined by agency management.

DISASTER RECOVERY: The process of restoring an AIS to full operation after an interruption in service, including equipment repair/replacement, file recovery/restoration, and resumption of service to users.

DISCLOSURE: Unauthorized access to confidential or sensitive information.

DISTRIBUTED COMPUTING ENVIRONMENT (DCE): A technology for managing heterogeneous client/server networks developed by the Open Software Foundation (OSF). It is a set of applications that provide common services, such as file sharing, security, and applications sharing for a variety of hardware platforms regardless of the underlying hardware, software, and operating systems.

DISTRIBUTED DoS ATTACK: Network-based attacks from many attack servers used remotely to send packets.

DMZ: De-militarized Zone. A network segment external to the university production network.

DNS SPOOFING: Assuming the DNS name of another system by either corrupting the name service cache of a victim system, or by compromising a domain name server for a valid domain.

DOMAIN: The unique context (e.g., access control parameters) in which a program is operating; in effect, the set of objects that a subject has the ability to access

DoS ATTACK: See Denial of Service Attack.

DSL: Digital Subscriber Line (DSL) is a form of high-speed Internet access competing with cable modems. DSL works over standard phone lines and supports data speeds of over 2 Mbps downstream (to the user) and slower speeds upstream (to the Internet).

DUAL HOMED GATEWAY: A dual homed gateway is a system that has two or more network interfaces, each of which is connected to a different network. In firewall configurations, a dual homed gateway usually acts to block or filter some or all of the traffic trying to pass between the networks. See Firewall.

DUAL HOMING: Having concurrent connectivity to more than one network from a computer or network device. Examples include: Being logged into the University network via a local Ethernet connection, and dialing into AOL or other Internet service provider (ISP). Being on a University of Texas at El Paso-provided Remote Access home network, and connecting to another network, such as a spouse's remote access. Configuring an ISDN router to dial into University of Texas at El Paso and an ISP, depending on packet destination.

eCOMMERCE MERCHANT: A department that processes online Web credit card payments or uses equipment that has an external facing IP address.

ELECTRONIC ATTACK (EA): That division of EW involving the use of electromagnetic, directed energy, or anti-radiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability. EA includes

actions taken to prevent or reduce an enemy's effective use of the electromagnetic spectrum, such as jamming and electromagnetic deception and employment of weapons that use either electromagnetic or directed energy as their primary destructive mechanism (lasers, radio frequency, or particle beams).

ELECTRONIC MAIL: See E-Mail

ELECTRONIC MAIL SYSTEM: Any computer software application that allows electronic mail to be communicated from one computing system to another.

ELECTRONIC MEDIA: Any of the following: a) Electronic storage media including storage devices in computers(hard drives, memory) and any removable/transportable digital storage medium, such as magnetic tape or disk, optical disk, or digital memory card; or b) Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the internet (wide-open), extranet (using internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, private networks, intranet, and the physical movement of removable/transportable electronic storage media.

ELECTRONIC PROTECTION (EP): That division of EW involving actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy employment of EW that degrade, neutralize, or destroy friendly combat capability.

ELECTRONIC WARFARE: Any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. The three major subdivisions within electronic warfare are electronic attack, electronic protection, and electronic warfare support.

ELECTRONIC WARFARE SUPPORT (ES): That division of EW involving actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition. Thus, electronic warfare support provides information required for immediate decisions involving EW operations and other tactical actions such as threat avoidance, targeting and homing. ES data can be used to produce signals intelligence.

E-MAIL: Any message, image, form, attachment, data, or other communication sent, received, or stored within an electronic mail system.

EMBEDDED SYSTEM: A system that performs or controls a function, either in whole or in part, as an integral element of a larger system or subsystem.

EMERGENCY CHANGE: When an unauthorized immediate response to imminent critical system failure is needed to prevent widespread service disruption.

EMISSION SECURITY: The protection resulting from all measures taken to deny unauthorized persons information of value that might be derived from intercept and from an analysis of compromising emanations from systems.

ENCAPSULATING SECURITY PAYLOAD (ESP): A mechanism to provide confidentiality and integrity protection to IP datagrams.

ENCRYPTED VIRUS: A virus whose code begins with a decryption algorithm, and continues with the scrambled or encrypted code of the remainder of the virus. When several identical files are infected with the same virus, each will share a brief identical decryption algorithm, but beyond that, each copy may appear different. A scan string could be used to search for the decryption algorithm. See Polymorphic Virus.

ENCRYPTING ROUTER: See Tunneling Router, Virtual Network Perimeter.

ENCRYPTION: The process of cryptographically converting plain text electronic data into a form unintelligible to anyone except the intended recipient.

ENTERPRISE NETWORK: A usually large, diverse network connecting most major points in an organization. Differs from WAN in that it is typically private and contained within a single organization.

ENTITLEMENT: The level of privilege that has been authenticated and authorized. The privileges level at which to access resources.

ENTITY: Any business unit, department, group, or third party, internal or external to University of Texas at El Paso, responsible for maintaining University of Texas at El Paso assets.

ENTITY WIDE SECURITY: Planning and management that provide a framework and continuing cycle of activity for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of the entity's physical and information system security controls. The program should establish a framework and continuing cycle of activity for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of these procedures. Without a well-designed program, security controls may be inadequate; responsibilities may be unclear, misunderstood, and improperly implemented; and controls may be inconsistently applied. Such conditions may lead to insufficient protection of sensitive or critical resources and disproportionately high expenditures for controls over low-risk resources.

ENTRAPMENT: The deliberate planting of apparent flaws in a system for the purpose of detecting attempted penetrations.

ENVIRONMENT: Aggregate of the external procedures, conditions, and objects affecting the development, operation, and maintenance of an AIS.

ENVIRONMENTAL SUPPORT: Includes clean air, heating and air conditioning, humidity, and water, some of which may be supplied or regulated by automated control systems.

EQUILIBRIUM: A state of balance existing between two or more opposing forces.

ETHERNET SNIFFING: Listening with software to the Ethernet interface for packets that interest the user. When the software sees a packet that fits certain criteria, it logs it to a file. The most interesting packet is one that contains words like login or password.

ETHICS: The principles of human morality and duty in an organization.

EVALUATE: To determine the amount or worth of or to appraise.

EVENT: An occurrence, not yet assessed, that may affect the performance of an AIS. See Incident.

EXE FILE: A PC-DOS executable file similar to a COM file, except that it is not restricted in size (except for memory limitations), and that it may contain relocatable code.

EXECUTING BODY: The series of computer instructions that the computer executes to run a program.

EXPOSURE: Vulnerability to loss resulting from accidental or intentional disclosure, modification, or destruction of information resources.

EXTRANET: An intranet that is accessible or partially accessible to authorized users outside the organization.

FALSE NEGATIVE: Occurs when an actual intrusive action has occurred but the system allows it to pass as non-intrusive behavior.

FALSE POSITIVE: Occurs when the system classifies an action as a possible intrusion when it is a legitimate action.

FAMILY API: An application-programming interface that allows a properly written program to work under both OS/2 and DOS. Family API programs have an OS/2 fork, which contains OS/2-specific code, and a DOS fork, which contains PC-DOS-specific code. In many cases, PC-DOS viruses that try to infect Family API applications get confused and end up damaging the program. Infected Family API applications often just do not work, rather than spread the infection. Some viruses infect executable files. There are a variety of mechanisms that they use to do so. Usually, the virus will get control when the program is first executed. In most cases, the virus will return control to the original program after it has completed its own execution.

FAQ: Frequently asked question(s).

FAULT: A condition that causes a device or system component to fail to perform in a required manner.

FAULT TOLERANCE: The ability of a system or component to continue normal operation despite the presence of hardware or software faults.

FEDERAL INFORMATION PROCESSING STANDARD (FIPS) PUBLICATION: A federal standard issued by the National Institute of Science and Technology (formerly the National Bureau of Standards). Each standard is assigned a number.

FILE PROTECTION: The aggregate of all processes and procedures in a system designed to inhibit unauthorized access, contamination, or elimination of a file.

FILE SECURITY: The means by which access to computer files is limited to authorized users only.

FILE SERVER: A computer containing files that may he shared by everyone connected to a LAN. A file server usually has software rules for allowing LAN users to get into and out of the files and databases it stores.

FILE TRANSFER: One of most popular network applications, whereby files can be moved from one network device to another.

FILE VIRUS: Viruses that attach themselves to (or replace) .COM and .EXE files, although in some cases they can infect files with extensions .SYS, .DRV, .BIN, .OVL, OVR, etc. The most common file viruses are resident viruses, going into memory at the time the first copy is run, and taking clandestine control of the computer. Such viruses commonly infect additional programs as you run them. But there are many nonresident viruses too, which simply infect one or more files whenever an infected file is run.

FIPS: See Federal Information Processing Standard Publication.

FIREWALL: An access control mechanism that acts as a barrier between two or more segments of a computer network or overall client/server architecture, used to protect internal networks or network segments from unauthorized users or processes.

FIRMWARE: Application recorded in permanent or semi-permanent computer memory.

FISHBOWL: To contain, isolate, and monitor an unauthorized user within a system in order to gain information about the user.

FISSEA: The Federal Information Systems Security Educator's Association, an organization whose members come from federal agencies, industry, and academic institutions devoted to improving the IT security awareness and knowledge within the federal government and its related external workforce.

FORK BOMB: Also known as Logic Bomb. Code that can be written in one line of code on any Unix system; used to recursively spawn copies of itself, "explodes" eventually, eating all the process table entries and effectively locks up the system.

FORMAL ACCESS APPROVAL: Documented approval by a data owner to allow access to a particular category of information.

FRAME: A group of bits sent over a communications channel, usually containing its own control information, including address and error detection.

FRAME RELAY: A method of communication that incrementally can go from the speed of an ISDN to the speed of a T1 line. Frame Relay has a flat-rate billing charge instead of a per time usage. Frame Relay connects via the telephone university's network.

FUNCTIONAL TESTING: The segment of security testing in which the advertised security mechanisms of the system are tested, under operational conditions, for correct operation.

GARDEN OF EDEN MECHANISM: A mechanism used only in the author's original copy of the virus and not in subsequent generations of it. It is sometimes possible to determine when a copy of a virus is the author's original copy by noticing that such a mechanism is functional. Also called a germ or generation one virus.

GATEWAY: Interface between networks that facilitate compatibility by adapting transmission speeds, protocols, codes, or security measures.

GENERAL SUPPORT SYSTEM: Interconnected information resources under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, facilities, and people, and provides support for a variety of users and/or applications. Individual applications support different mission-related functions. Users may be from the same or different organizations.

GENERALLY ACCEPTED SYSTEM SECURITY PRINCIPLES (GSSP): The practices, conventions, miles, mechanisms, and procedures that information security professionals should employ, or that information processing products should provide, to achieve, preserve, and restore the properties of integrity, availability, and confidentiality of information and information systems at a particular time.

GRAPHICAL USER INTERFACE (GUI) DISPLAY: The display of intrusion detection information that appears on the system administrator's console.

HACKER: Any unauthorized user who gains, or attempts to gain, access to an AIS, regardless of motivation.

HACKING: Unauthorized use or attempts to circumvent or bypass the security mechanisms of an information system or network.

HACKING RUN: A hack session extended long outside normal working times, especially one longer than 12 hours.

HALON: A gas used to extinguish fires effective only in closed areas.

HANDSHAKING PROCEDURE: A dialogue between two entities (e.g., a user and a computer, a computer and another computer, or a program and another program) for the purpose of identifying and authenticating the entities to one another.

HARDWARE: The physical components of a computer system such as computers, printers, disks, interface cards, and other physical equipment.

HASH: An algorithmically generated number that identifies a datum or its location.

HETEROGENEOUS: Assorted, varied, and diverse.

HIGH INTEGRITY COMPUTING LABORATORY (HICL): The group at the IBM Thomas J. Watson Research Center responsible for IBM Antivirus research and development. The group carries out studies of viral spread and behavior, and develops customer solutions.

HIJACKING: An attack that occurs during an authenticated session with a database or system. The attacker disables a user's desktop system, intercepts responses from the application, and responds in ways that prolong the session.

HOST: A computer system that provides computer service for a number of users.

HOST TO FRONT-END PROTOCOL: A set of conventions governing the format and control of data passed from a host to a front-end machine.

HOST-BASED: Information, such as audit data from a single host, which may be used to detect intrusions

HOST-BASED SECURITY: The technique of securing an individual system from attack. Host-based security is operating system and version dependent.

HOT SITE: An alternate site with a duplicate AIS already set up and running, maintained by an organization or its contractor to ensure continuity of service for critical systems in the event of a disaster. See Cold Site.

HUB: A hardware/software device that contains multiple independent but connected modules of network and internetwork equipment. Hubs may be active, where they repeat signals sent through them, or passive, where they do not repeat, but merely split, signals sent through them.

IA: See Information Assurance.

IBM ANTIVIRUS: IBM's premiere anti-virus software for DOS, Windows, Windows 95, Windows NT, OS/2 and Novell NetWare. It is a standard part of IBM Antivirus Services. Versions are available for use on individual PCs, for installation on client PCs from network servers, and for execution on client PCs from network servers.

ICMP: See Internet Control Message Protocol.

IDEA (INTERNATIONAL DATA ENCRYPTION ALGORITHM): A private key encryption-decryption algorithm that uses a key that is twice the length of a DES key.

IDENTIFICATION: The process that enables, generally by the use of unique machine-readable names, recognition of users or resources as identical to those previously described to an AIS.

IDIOT: Intrusion Detection in our Time. A system that detects intrusions using pattern matching.

IDS: See Intrusion Detection System.

IMPACT: Effect of one thing on another.

IN THE WILD VIRUS: A term that indicates that a virus has been found in several organizations somewhere in the world. It contrasts the virus with one that has only been reported by researchers. Despite popular hype, most viruses are "in the wild" and differ only in prevalence. Some are new and therefore extremely rare. Others are old, but do not spread well, and are therefore extremely rare.

INCIDENT: A successful or unsuccessful action attempting to circumvent technical controls, organizational policy, or law. This is often called an attack. See Controls, Information Mining, Insider Attack, Intrusion Detection, Malicious Software, Policy, Social Engineering, Spoofing.

INCOMPLETE PARAMETER CHECKING: A system design flaw that results when all parameters have not been fully anticipated for accuracy and consistency, thus making the system vulnerable to penetration.

INDIVIDUAL ACCOUNTABILITY: Requires individual users to be held accountable for their actions after being notified of the rules of behavior in the use of the system and the penalties associated with the violation of those rules.

INFORMATION: That which is extracted from a compilation of data in response to a specific need.

INFORMATION ASSURANCE (IA): Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

INFORMATION ATTACK: An attempt to bypass the physical or information security measures and controls protecting an Information Resource. The attack may alter, release, or deny data. Whether an attack will succeed depends on the vulnerability of the computer system and the effectiveness of existing countermeasures.

INFORMATION MINING: Acquiring information about systems, networks, or users that will aid in formulating other attacks. See Incident.

INFORMATION OPERATIONS (IO): Actions taken to affect adversary information and information systems while defending one's own information and information systems.

INFORMATION RESOURCES (IR): Any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistant (PDA), pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

INFORMATION RESOURCES AND PLANNING (IRP): The name of the agency department responsible for computers, networking and data management. The scientific, technological, and engineering disciplines and the management technologies used in information handling, communication, and processing; the fields of electronic data processing, telecommunications, networks, and their convergence in systems; applications and associated software and equipment together with their interaction with humans and machines.

INFORMATION RESOURCES MANAGER (IRM): The person designated by the head of each state agency to have oversight responsibility for all information resources within the agency. Responsible to the State of Texas for management of the agency's information resources. The designation of an agency information resources manager is intended to establish clear accountability for setting policy for information resources management activities, provide for greater coordination of the state agency's information activities, and ensure greater visibility of such activities within and between state agencies. The IRM has been given the authority and the accountability by the State of Texas to implement Security Policies, Procedures, Practice Standards, and Guidelines to protect the Information Resources of the agency. If an agency does not designate an IRM, the title defaults to the agency's Executive Director, and the Executive Director is responsible for adhering to the duties and requirements of an IRM.

INFORMATION SECURITY: Technological discipline concerned with ensuring that information systems perform as expected and do nothing more; that information is adequately protected for confidentiality; that system, data and software integrity is maintained; and that information and system resources are protected against unplanned disruptions of processing that could seriously impact mission accomplishment. The result of any system of policies and/or procedures for identifying, controlling, and protecting from unauthorized disclosure, information whose protection is authorized by executive order or statute. See Automated Information System Security, Computer Security, and Information Systems Security.

INFORMATION SECURITY BASICS: A core set of generic information security terms and concepts for all federal employees as a baseline for further, role-based learning.

INFORMATION SECURITY BODY OF KNOWLEDGE TOPICS AND CONCEPTS: A set of 12 high-level topics and concepts intended to incorporate the overall body of knowledge required for training in information security.

INFORMATION SECURITY FUNCTION: The elements, structure, objectives, and resources needed to establish an agency level security program. Its role is to provide leadership to the agency information processing community in the areas of information security, integrity, and privacy.

INFORMATION SECURITY LITERACY: The first solid step of information security training where the knowledge obtained through training can be directly related to the individual's role in his or her specific organization.

INFORMATION SECURITY OFFICER (ISO): The person designated to administer the agency's information security program. Responsible to the IRM for administering the information security functions within the agency. The ISO is the agency's internal and external point of contact for all information security matters.

INFORMATION SECURITY POLICY: The set of rules and practices an agency uses to manage and protect its information resources

INFORMATION SECURITY PROGRAM: A program established, implemented, and maintained to assure that adequate information security is provided for all organizational information collected, processed, transmitted, stored, or disseminated in its information technology systems. See Computer Security Program, Information Systems Security Program.

INFORMATION SHARING: The requirements for information sharing by an AIS system with one or more other AIS systems or applications, for information sharing to support multiple internal or external organizations, missions, or public programs.

INFORMATION SUPERIORITY: The capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same.

INFORMATION SYSTEM RESOURCES: A collection of computing and/or communications components and other resources that support one or more functional objectives of an organization. Information system resources include any component plus associated manual procedures and physical facilities that are used in the acquisition, storage, manipulation, display, and/or movement of data or to direct or monitor operating procedures. An information system may consist of one or more computers and their related resources of any size. The resources that comprise a system do not have to be physically connected.

INFORMATION SYSTEM (IS): All the electronic and human components involved in the collection, processing, storage, transmission, display, dissemination, and disposition of information. An AIS may be automated (e.g., a computerized information system) or manual (e.g., a library's card catalog). See AIS.

INFORMATION SYSTEMS SECURITY (INFOSEC): A composite of means to protect telecommunications systems and automated information systems and the information they process.

INFORMATION SYSTEMS SECURITY PROGRAM: Synonymous with Information Security Program. Information technology computing and/or communications hardware and/or software components and related resources that can collect, store, process, maintain, share, transmit, or dispose of data. IRP components include computers and associated peripheral devices, computer operating systems, utility/support software, and communications hardware and software. See Information Resources and Planning (IRP), Information Security.

INFORMATION TECHNOLOGY (IT): See Information Resources and Planning (IRP)

INFORMATION WARFARE (IW): Information operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries.

INFOSEC: See Information Systems Security.

INSIDER ATTACK: An attack originating from inside a protected network. See Incident.

INTANGIBLE: Incapable of being perceived by touch.

INTEGRITY: The accuracy and completeness of information and assets and the authenticity of transactions.

INTEGRITY SERVICE: In cryptography, a service that guarantees that the message has not been modified since it was signed by the message originator.

INTERFACE: A connection between two systems or devices. A demarcation between two devices where the electrical signals, connectors, timing, and handshaking meet. Also, the boundary between adjacent layers of the OSI model.

INTERNAL CONTROL: The templating of access to a particular data element or set, by an agency instrumentality, in accordance with law, code, or policy. If that data element or set is shared with another agency, the originating agency's internal control policy applies to the receiving agency.

INTERNAL SECURITY CONTROLS: Hardware, firmware, and software features within a system that restrict access to resources (hardware, software, and data) to authorized subjects only (persons, programs, or devices).

INTERNAL USE: The classification of data that does not require any degree of protection against disclosure within the company (operating procedures, policies, and standards; interoffice memo; company phone directory).

INTERNET: A global system interconnecting computers and computer networks. The computers and networks are owned separately by a host of organizations, government agencies, companies, and colleges. The Internet is the present "information super highway."

INTERNET CONTROL MESSAGE PROTOCOL: An error reporting protocol capable of handling several types of error conditions and reporting errors back to its original source. It is also used to restrain hosts that are sending too many packets and to measure network performance using ECHO_REQUEST/REPLY and TIMESTAMP REQUEST/REPLY messages. In addition ICMP messages are used to allow hosts to discover network numbers.

INTERNET PROTOCOL (IP): A communications protocol that routes packets of data. The address of the destination system is used by intermediate routers to select a path through the network. See Transmission Control Protocol. Internet Worm: A worm program (see Worm) that was unleashed on the Internet in 1988. It was written by Robert T. Morris as an experiment that got out of hand.

INTEROPERABILITY: The ability of software to operate on a variety of platforms.

INTRANET: A private network for communications and sharing of information that, like the Internet, is based on TCP/IP, but is accessible only to authorized users within an organization. An organization's intranet is usually protected from external access by a firewall. See Extranet.

INTRUSION: Any set of actions that attempt to compromise the integrity, confidentiality or availability of a resource.

INTRUSION DETECTION: Pertaining to techniques that attempt to detect intrusion into a computer or network by observation of actions, security logs, or audit data. Detection of break-ins or attempts either manually or via= software expert systems that operate on logs or other information available on the network.

INTRUSION DETECTION SYSTEM (IDS): A software package that collects information from a variety of system and network sources, analyzes the information stream for signs of misuse (attacks originating within the system or network) or intrusion (attacks or attempted attacks from outside), and reports the outcome of the detection process.

IP SPLICING/HIJACKING: An action whereby an active, established, session is intercepted and co-opted by the unauthorized user. IP splicing attacks may occur after an authentication has been made, permitting the attacker to assume the role of an already authorized user. Primary protections against IP splicing rely on encryption at the session or network layer.

IP SPOOFING: An attack whereby a system attempts to illicitly impersonate another system by using its IP network address. See Spoofing.

IPSEC CONCENTRATOR: A device in which VPN connections are terminated.

IRM: See Information Resources Manager.

IRP: Information Resources and Planning

IS: Information system.

ISDN: There are two flavors of Integrated Services Digital Network or ISDN: BRI and PRI. BRI is used for home office/remote access. BRI has two "Bearer" channels at 64kbit (aggregate 128kb) and 1 D channel for signaling info.

ISO: See Information Security Office.

ISOLATION: The containment of subjects and objects in a system in such a way that they are separated from one another, as well as from the protection controls of the operating system.

ISSUE-SPECIFIC POLICY: Addresses issues of current relevance and concern to the agency. Issue-specific policy statements are likely to be limited, particular, and rapidly changing. Their promulgation may be triggered by a computer security incident.

IT: See Information Resources and Planning (IRP).

KERBEROS: Authentication that validates users through a system that keeps the actual identity of the user out of the network communication- where it could be easily intercepted and duplicated-and keeps it in encrypted files.

KEY: A symbol or sequence of symbols (or electrical or mechanical correlates of symbols) applied to text in order to encrypt or decrypt.

KEY BACKUP AND RECOVERY: Secure means for backup and recovery of encryption key pairs.

KEY ESCROW: The system of giving a piece of a key to each of a certain number of trustees such that the key can be recovered with the collaboration of all the trustees.

KEY HISTORIES: The transparent association of old key pairs with data encrypted by those keys.

KEYS: Strings of bits used in conjunction with algorithms to make the required transformations in encryption.

KEYSTROKE MONITORING: A specialized form of audit trail software, or a specially designed device, that records every key struck by a user and every character of the response that the AIS returns to the user.

KNOWLEDGE BASES: Provide the means for creating user and system normal/abnormal activity profiles, capturing and storing new attack signatures, and storing any other information useful for intrusion detection.

LAB NETWORK: A "lab network" is defined as any network used for the purposes of testing, demonstrations, training, etc. Any network that is stand-alone or fire walled off from the production network(s) and whose impairment will not cause direct loss to the University of Texas at El Paso nor affect the production network.

LAN: See Local Area Network.

LAPTOP COMPUTER: A portable computer usually powered by a rechargeable battery. The smaller versions are also called notebook computers.

LAWS AND REGULATIONS: Federal government-wide and organization-specific laws, regulations, policies, guidelines, standards, and procedures mandating requirements for the management and protection of information technology resources.

LDAP: Lightweight **D**irectory **A**ccess **P**rotocol, a set of protocols for accessing information directories.

LEAPFROG ATTACK: Use of userid and password information obtained illicitly from one host to compromise another host. The act of TELNETing through one or more hosts in order to preclude a trace (a standard cracker procedure).

LEARNING CONTINUUM: A representation in which the common characteristic of learning is presented as a series of variations from awareness through training to education.

LEARNING OBJECTIVE: A link between "knowledge levels" and "behavioral outcomes" that provides examples of the activities an individual should be capable of doing after successful completion of training. Learning objectives recognize that training must be provided at beginning, intermediate, and advanced levels.

LEASED LINE: A transmission line reserved by a communications carrier for the private use of a customer.

LEAST PRIVILEGE: This principle requires that each subject in a system be granted the most restrictive set of privileges (or lowest clearance) needed for the performance of authorized tasks. The application of this principle limits the damage that can result from accident, error, or unauthorized use.

LETTER BOMB: A piece of e-mail containing live data intended to do malicious things to the recipient's machine or terminal. Under UNIX, a letter bomb can also try to get part of its contents interpreted as a shell command to the mailer. The results of this could range from silly to denial of service.

LIKELIHOOD: The state or quality of being probable, probability.

LIKERT SCALE: An evaluation tool that is usually from one to five (one being very good, five being not good, or vice versa), designed to allow an evaluator to prioritize the results of the evaluation.

LINK: Network communications channel consisting of a circuit or transmission path, including all equipment, between a sender and a receiver. Most often used to refer to a LAN or WAN connection.

LOCAL AREA NETWORK (LAN): A data communications network spanning a limited geographical area, a few miles at most. It provides communication between computers and peripherals at relatively high data rates and relatively low error rates.

LOCAL ATTACK: A local attack can be a program that creates an infinite loop, makes many copies of itself, and continues to open many files.

LOG PROCESSING: How audit logs are analyzed, consolidated, reduced, searched for key events, stored, or summarized.

LOG RETENTION: How long audit logs are retained and maintained.

LOGGING: The process of storing information about events that occurred on the firewall, host system, or network. This process creates audit logs.

LOGIC BOMB: A small, malicious program that is activated by a trigger (such as a date or the number of times a file is accessed), usually to destroy data or source code. See Virus.

MACRO VIRUS: A virus that consists of instructions in Word Basic or some other macro language, and resides in a document. While we do not think of documents as capable of being infected, any application that supports automatically executable macros is a potential platform for macro viruses. Because documents are now even more widely shared than diskettes (through networks and the Internet), document-based viruses are likely to dominate our future.

MAGNETIC REMANENCE: A measure of the magnetic flux density remaining after removal of the applied magnetic force. Refers to any data remaining on magnetic storage media after removal of the power.

MAIL BOMB: The mail sent to urge others to send massive amounts of e-mail to a single system or person, with the intent to crash the recipient's system. Mail bombing is widely regarded as a serious offense.

MAINTENANCE HOOK: Special instructions in software to allow easy maintenance and additional feature development. These are not clearly defined during access for design specification. Hooks frequently allow entry into the code at unusual points or without the usual checks, so they are a serious security risk if they are not removed prior to live implementation. Maintenance hooks are special types of trap doors.

MAJOR APPLICATION: An application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. A breach in a major application might comprise many individual application programs and hardware, software, and telecommunications components. Major applications can be either a major software application or a combination of hardware/software where the only purpose of the system is to support a specific mission-related function.

MALICIOUS CODE: Any program or piece of code designed to do damage to a system or the information it contains, or to prevent the system from being used in its normal manner.

MALICIOUS PROGRAM: Source code incorporated into an application that directs an AIS to perform an unauthorized, often destructive, action.

MALICIOUS SOFTWARE: Software which damages a system/network or circumvents a system's/network's technical controls or takes other illicit action. See Incident, Trojan horse, and Virus.

MANAGEMENT CONTROLS: Management controls are actions taken to manage the development, maintenance, and use of the system, including system-specific policies, procedures, and rules of behavior, individual roles and responsibilities, individual accountability, and personnel security decisions.

MASQUERADING: See Spoofing.

MASTER BOOT RECORD: The 340-byte program located in the master boot sector. This program begins the boot process. It reads the partition table, determines what partition will be booted from (normally C:), and transfers control to the program stored in the first sector of that partition, which is the boot sector. The master boot record is often called the MBR, master boot sector, or partition table. It is created when FDISK or FDISK /MBR is run.

MASTER BOOT SECTOR: The first sector of the hard disk to be read. This sector is located on the top side (side 0), outside cylinder (cylinder 0), first sector (sector 1). The sector contains the master boot record.

MASTER BOOT SECTOR VIRUS: A virus that infects the master boot sector, such as NYB, spreads through the boot sector of floppy disks. If you boot or attempt to boot your system with an infected floppy disk, NYB loads into memory and then writes itself to the master boot sector on the hard drive. If the disk is not bootable, you see the DOS error message "Non-system disk or disk error..." If the disk is bootable, the system boots to the A: prompt. Regardless of the way the system is infected, there is no indication on the screen that this has happened. Once the hard drive is infected, NYB loads into memory each time the system is booted. The virus stays in memory, waiting for DOS to access a floppy disk. It then infects the boot record on each floppy DOS accesses.

MEDIA: Short for storage media. Physical objects on which data can be stored, such as hard disks, CD-ROMs, floppy disks, and tapes.

MEI: See Minimum Essential Infrastructure.

MEMORY: A computer's internal capacity to store data determined by the microchips installed.

MERCHANT: University unit that accepts credit card payment for goods, services, or gifts.

MERCHANT ACCOUNT: A credit card account number assigned by the credit card processor, Global Payments, etc., to permit credit card payment processing.

METRIC: A random variable x representing a quantitative measure accumulated over a period.

MIMICKING: Synonymous with Masquerading, Spoofing.

MINIMUM ESSENTIAL INFRASTRUCTURE: The components of an IT strategy that the enterprise cannot do without and that must be accommodated in its security strategy.

MINIMUM LEVEL OF PROTECTION: The reduction in the total risk that results from the impact of in-place safeguards. See Total Risk, Acceptable Risk, Residual Risk.

MISSION CRITICAL INFORMATION RESOURCES: Information Resources defined by an institution of higher education or state agency to be essential to the Entity's function and which if made unavailable will inflict substantial harm to the Entity and the Entity's ability to meet its instructional, research, patient care, or public service missions. Mission Critical Information Resources include Confidential Data and Sensitive Data.

MISUSE DETECTION MODEL: The system detects intrusions by looking for activity that corresponds to a known intrusion technique or system vulnerability. Also known as Rules-Based Detection.

MITIGATE: To do something to reduce the risk to an acceptable level.

MOCKINGBIRD: A computer program or process that mimics the legitimate behavior of a normal system feature (or other apparently useful function) but performs malicious activities once invoked by the user.

MODEM: Acronym for modulator-demodulator. A device or application that permits a computer to transmit data over telephone lines by converting digital data to an analog signal.

MODULE: A collection of computer language instructions grouped together either logically or physically. A module may also be called a package or a class, depending upon which computer language is used.

MULTIHOST-BASED AUDITING: Audit data from multiple hosts may be used to detect intrusions.

MULTILEVEL SECURE: A class of system containing information with different sensitivities that simultaneously permits access by users with different security clearances and need-to-know, but prevents users from obtaining access to information for which they lack authorization.

MULTILEVEL SECURE MODE: A mode of operation that allows two or more classification levels of information to be processed simultaneously within the same system when not all

users have a clearance, authorization, or formal access approval for all information handled by the AIS.

MULTIPARTITE VIRUS: A multipartite virus infects boot sectors and files. Often, an infected file is used to infect the boot sector; thus, this is one case where a boot sector infector could spread across a network.

MULTIPLE ACCESS RIGHTS TERMINAL: A terminal that may be used by more than one class of users; for example, users with different access rights to data.

MULTIPLEXING: The transmission of multiple signals over a single communications line.

MULTISTATION ACCESS UNIT (MAU): A wiring concentrator to which token ring lobes attach.

MULTI-USER MODE OF OPERATION: A mode of operation designed for systems that process sensitive unclassified information in which users may not have a need-to-know for all information processed in the system. This mode is also for microcomputers processing sensitive unclassified information that cannot meet the requirements of the stand-alone mode of operation.

NAK ATTACK: Negative acknowledgment. A penetration technique that capitalizes on a potential weakness in an operating system that does not handle asynchronous interrupts properly and thus leaves the system in an unprotected state during such interrupts.

NAME SPACE: A logical area of code in which the declared symbolic names are known and outside of which these names are not visible.

NATIONAL INFORMATION INFRASTRUCTURE (NII): The nationwide interconnection of communications networks, computers, databases, and consumer electronics that make vast amounts of information available to users. The NII encompasses a wide range of equipment, including cameras, scanners, keyboards, facsimile machines, computers, switches, compact disks, video and audio tape, cable, wire, satellites, and fiber-optic transmission lines, networks of all types, monitors, printers and much more. The friendly and adversary personnel who make decisions and handle the transmitted information constitute a critical component of the NII.

NEED-TO-KNOW: The necessity for access to, knowledge of, or possession of specific information required to carry out official duties.

NETWARE: A LAN operating system from Novell, Inc., Orem, Utah.

NETWORK: All associated equipment and media creating electronic transmission between any information resource(s), such as wired, optical, wireless, IP, synchronous serial, telephony, etc. **NETWORK FRONT END:** A device that implements the necessary network protocols, including security-related protocols, to allow a computer system to be attached to a network.

NETWORK LAYER: The third layer of the OSI model of data communications. It involves routing data messages through the network using alternative routes.

NETWORK MEDIA: Plural of medium. The physical environment through which transmission signals pass. Common network media include twisted pair, coaxial, and fiber optic cable, and the atmosphere (microwave, infrared transmission).

NETWORK OPERATING SYSTEM (NOS): The software used to connect devices, share resources, transfer files and perform network activity. Usually, there are two parts to a network operation system: server and workstation (requester).

NETWORK PROTOCOL: (1) A formal set of conventions governing the format and control of interactions between communicating functional modules. (2) The OSI network layer specifies a protocol that provides the functional and procedural means of transferring variable length data sequences from a source to a destination via one or more networks while maintaining the quality of service requested by the node.

NETWORK SECURITY: Security procedures and controls that protect a network from (1) unauthorized access, modification, and information disclosure and (2) physical impairment or destruction.

NETWORK SECURITY OFFICER: Individual formally appointed by a designated approving authority to ensure that the provisions of all applicable directives are implemented throughout the life cycle of an automated information system network.

NETWORK TOPOLOGY: The architectural layout of a network. Common topologies include bus (nodes connected to a single backbone cable), ring (nodes connected serially in a closed loop), and star (nodes connected to a central hub). See Network.

NETWORK TRUSTED COMPUTING BASE (NTCB): The totality of protection mechanisms within a network system- including hardware, firmware, and software-the combination of which is responsible for enforcing a security policy. The NTCB is the network generalization of the trusted computing base (TCB).

NETWORK WEAVING: Another name for "leapfrogging."

NETWORK-BASED: Network traffic data along with audit data from the hosts used to detect intrusions.

NETWORK-BASED ATTACK: These attacks can tie up system resources, crash a system, and flood a network.

NETWORK-LEVEL FIREWALL: A firewall in which traffic is examined at the network protocol (IP) packet level.

NETWORKS: Include communication capability that allows one user or system to connect to another user or system and can be part of a system or a separate system. Examples of

networks include local area networks or wide area networks, including public networks such as the Internet.

NIST: National Institute of Standards and Technology-federal standards organization within U.S. Department of Commerce that ensures standardization among government agencies.

NODES: Points in a network where service is provided used, or where communications channels are interconnected.

NON-eCOMMERCE MERCHANT: A department that processes credit card payments with equipment that does not utilize an external facing IP address, such as point-of-sale terminals, cash registers and other types of equipment.

NONREPUDIATION: Method by which the sender of data is provided with proof of delivery and the recipient is assured of the sender's identity, so that neither can later deny having processed the data.

ON-DEMAND SCANNING: Synonymous with offline, manual scanning, foreground, nonresident scanning, scanning.

ONLINE TRANSACTION PROCESSING (OLTP): The high-end of transaction oriented DBMS applications.

OPEN ARCHITECTURE: An architecture to which third-party developers can legally develop products and for which public domain specifications exist.

OPEN RECORDS: Any record that is NOT subject to the Public Records Act or other federal or state legal restrictions.

OPEN SECURITY ENVIRONMENT: An environment that includes those systems in which at least one of the following conditions holds true: 1) application developers (including maintainers) do not have sufficient clearance or authorization to provide an acceptable presumption that they have not introduced malicious logic; 2) configuration control does not provide sufficient assurance that applications are protected against the introduction of malicious logic prior to and during the operation of system applications.

OPEN SOFTWARE FOUNDATION (OSF): A nonprofit organization based in Cambridge, MA. OSF represents more than 200 computer industry manufacturers who banded together to create a standard for tying together a common network.

OPEN SYSTEM: A system with specified nonproprietary standards that enable it to be readily connected to other systems.

OPEN SYSTEMS INTERCONNECTION (OSI) REFERENCE MODEL: The ISO has established the OSI model. The idea of OSI is to provide a network architectural model to allow equipment from different vendors to communicate. It is also used to teach and understand network functionality. The model defines and describes seven layers-(7) application, (6) presentation, (5) session, (4) transport, (3) network, (2) data link, (1) physical.

OPEN SYSTEMS SECURITY: Provision of tools for the secure internetworking of open systems.

OPERATING SYSTEM: Software required by every computer that (1) enables it to perform basic tasks such as controlling disks, drives, and peripheral devices; and (2) provides a platform on which applications can run.

OPERATIONAL CONTROLS: The day-to-day procedures and mechanisms used to protect operational systems and applications. Operational controls affect the system and application environment.

OPERATIONAL DATA SECURITY: The protection of data from either accidental or unauthorized, intentional modification, destruction, or disclosure during input, processing, or output operations.

OPERATIONS SECURITY (OPSEC): (1) The process of denying adversaries information about friendly capabilities and intentions by identifying, controlling, and protecting indicators associated with planning and conducting military operations and other activities. (2) An analytical process by with the U.S. government and its supporting contractors can deny to potential adversaries information about capabilities and intentions by identifying, controlling, and protecting evidence of the planning and\ execution of sensitive activities and operations.

OPTICAL SCANNER: A peripheral device that can read printed text or illustrations and translate them into a digitized image (bit map) that can be stored, displayed, and manipulated on a computer.

OS/2: An operating system sold by IBM for IBM PCs, and compatible computers. It is a multi-tasking operating system, which can run many PC-DOS and Windows programs.

OSI: Open Systems Interconnection. A set of internationally accepted and openly developed standards that meet the needs of network resource administration and integrated network utility.

OWNER: The authoritative head of the respective college, school, or unit. The owner is responsible for the function that is supported by the resource or for carrying out the program that uses the resources. The owner of a collection of information is the person responsible for the business results of that system or the business use of the information. Where appropriate, ownership may be shared by managers of different departments. The owner or his designated representatives are responsible for and authorized to:

- Approve access and formally assign custody of an information resources asset.
- Determine the asset's value.
- Specify and establish data control requirements that provide security, and convey them to users and custodians.
- Specify appropriate controls, based on risk assessment, to protect the state's information resources from unauthorized modification, deletion, or disclosure. Controls shall extend to information resources outsourced by the university.
- Confirm that controls are in place to ensure the accuracy, authenticity, and integrity of data.

- Confirm compliance with applicable controls.
- Assign custody of information resources assets and provide appropriate authority to implement security controls and procedures.
- Review access lists based on documented security risk management decisions.

PACKET: A block of data sent over the network transmitting the identities of the sending and receiving stations, error-control information, and message.

PACKET FILTER: A type of firewall that examines each packet and accepts or rejects it based on the security policy programmed into it in the form of rules.

PACKET FILTERING: A feature incorporated into routers and bridges to limit the flow of information based on pre-determined communications such as source, destination, or type of service being provided by the network. Packet filters let the administrator limit protocol-specific traffic to one network segment, isolate e-mail domains, and perform many other traffic control functions.

PACKET FILTERING FIREWALL: Consists of a screening router and a set of rules that accept or reject a message based on information in the message's header (a packet): the source address, destination address, and port.

PACKET INTERNET GOPHER: A program used to test whether a particular network destination is online, by sending an Internet control message protocol (ICMP) echo request and waiting for a response. Also called a Ping.

PACKET SNIFFER: A device or program that monitors the data traveling between computers on a network.

PACKET SWITCHING: A data transmission method, using packets, whereby a channel is occupied only for the duration of transmission of the packet. The packet switch sends the different packets from different data conversations along the best route available in any particular order. In contrast, a circuit-switching network dedicates one circuit at a time to data transmission.

PARTITIONED MODE: A mode of operation in which all persons have the clearance, but not necessarily the need-to-know and formal access approval, for all data handled by the AIS.

PASSIVE ATTACK: Attack that does not result in an unauthorized state change, such as an attack that only monitors and/or records data.

PASSIVE THREAT: The threat of unauthorized disclosure of information without changing the state of the system. A type of threat that involves the interception, not the alteration, of information.

PASSWORD: A string of characters used to verify or “authenticate” a person’s identity.

PASSWORD CRACKER: An application that tests for passwords that can be easily guessed, such as words in the dictionary or simple strings of characters (e.g., "abcdefgh" or "qwertyuiop").

PATCH: A modification to software that fixes an error in an application already installed on an AIS, generally supplied by the vendor of the software.

PC: Personal computer.

PC-DOS: An operating system sold by IBM for the IBM PC and compatible computers. Microsoft Corp. produces a functionally similar version of this operating system called MS-DOS. Viruses that infect PC-DOS systems almost always infect MS-DOS systems, and vice versa.

PEER-TO-PEER COMPUTING: As contrasted with client/server computing, peer-to-peer computing calls for each network device to run both client and server portions of an application.

PEM (PRIVACY ENHANCED MAIL): An IETF standard for secure electronic mail exchange.

PENETRATION: The successful unauthorized access to an automated system.

PENETRATION SIGNATURE: The description of a situation or set of conditions in which a penetration could occur or of system events which in conjunction can indicate the occurrence of a penetration in progress.

PENETRATION STUDY: A study to determine the feasibility and methods for defeating controls of a system.

PENETRATION TESTING: The portion of security testing in which the evaluators attempt to circumvent the security features of a system. The evaluators may be assumed to use all system design and implementation documentation, which may include listings of system source code, manuals, and circuit diagrams. The evaluators work under the same constraints applied to ordinary users.

PERFORMANCE-BASED: A method for designing learning objectives based on behavioral outcomes rather than on content, that provides benchmarks for evaluating learning effectiveness.

PERIMETER-BASED SECURITY: The technique of securing a network by controlling access to all entry and exit points of the network. Usually associated with firewalls and/or filters.

PERIODS PROCESSING: A security mode of operation and/or maximum classification of data handled is established for an interval of time, and then changed for the following interval of time. The period extends from the time when the system is securely initialized to the time when the system is purged of all sensitive data handled during the processing period.

PERIPHERAL EQUIPMENT: Any external device attached to a computer, including monitors, keyboards, mice, printers, optical scanners, and the like.

PERMISSIONS: A description of the type of authorized interactions a subject can have with an object. Examples include: read, write, execute, add, modify, and delete.

PERPETRATOR: The entity from the external environment that is taken to be the cause of a risk. An entity in the external environment that performs an attack, i.e., hacker.

PERSONAL IDENTIFIER OR USER IDENTIFICATION CODE: DATA item associated with a specific individual, representing the identity of that individual and possibly known by other individuals.

PERSONNEL SECURITY: The procedures established to insure that all personnel who have access to any sensitive information have the required authorities as well as all appropriate clearances.

PERVASIVE PRINCIPLES: The general approach information security should take to establish, maintain, and report on the security of systems in order to assure data integrity, availability, and confidentiality. There are seventeen drafted principles addressing issues of accountability, awareness, ethics, multidisciplinary, proportionality, integration, timeliness, reassessment, democracy, certification and accreditation, internal control, adversary, least privilege, separation of duty, continuity, simplicity, and policy-centered security.

PGP (PRETTY GOOD PRIVACY): A freeware program primarily for secure electronic mail.

PHAGE: A program that modifies other programs or databases in unauthorized ways, especially one that propagates a virus or Trojan horse.

PHF: Phone book file demonstration program that hackers use to gain access to a computer system and potentially read and capture password files.

PHF HACK: A well-known and vulnerable CGI script that does not filter out special characters (such as a new line) input by a user.

PHRACKER: An individual who combines phone phreaking with computer hacking.

PHREAK(ER): An individual fascinated by the telephone system. Commonly, an individual who uses his knowledge of the telephone system to make calls at the expense of another.

PHREAKING: The art and science of cracking the phone network.

PHYSICAL SECURITY: (1) The measures used to provide physical protection of resources against deliberate and accidental threats. (2) The protection of building sites and equipment (and information and software contained therein) from theft, vandalism, natural and manmade disasters, and accidental damage.

PIGGYBACK: The gaining of unauthorized access to a system via another user's legitimate connection.

PING OF DEATH: The use of ping with a packet size higher than 65,507. This will cause a denial of service.

PING REQUESTS: A program used to test whether a particular network destination is online, by sending an Internet control message protocol (ICMP) echo request and waiting for a response. Synonymous with Packet Internet Gopher).

PKI: See Public Key Infrastructure.

PLAINTEXT: Unencrypted data.

PLATFORM: The foundation technology of a computer system. The hardware and systems software that together provide support for an application program.

POLICY: Organization-level rules governing acceptable use of computing resources, security practices, and operational procedures.

POLYMORPHIC VIRUSES: A self-garbling virus whose degarbling header changes each time it spreads. These viruses are intended to be difficult to detect, though this is rarely the case in practice.

PORTABLE COMPUTING DEVICES: Any easily portable device that is capable of receiving and/or transmitting data to and from IR. These include, but are not limited to, notebook computers, handheld computers, PDAs, pagers, and cell phones.

POSITION OF SPECIAL TRUST: A position of special trust is one in which the individual can view confidential information, alter sensitive information or is depended upon for the continuity of Information Resources that are determined to be essential. A person is also considered to be in a position of special trust if that person acts independently of controls and supervision and impacts the confidentiality, integrity, or availability of confidential or sensitive information.

PRIVATE KEY CRYPTOGRAPHY: An encryption methodology in which the encryptor and decryptor use the same key, which must be kept secret. This methodology is usually only used by a small group.

PRIVATE LINE: A dedicated line leased from a common carrier.

PROBABILITY: The likelihood, in a finite sample, that an event will occur or a specific loss will happen. For example, once every 3 years carries a .33 probability; once every 30 years carries a .033 probability.)

PROBE: A device programmed to gather information about an AIS or its users.

PROCEDURAL SECURITY: See Administrative Security.

PROCEDURE: Step-by-step instructions followed in order to perform a task or meet a given standard.

PROCESS: A sequence of steps performed for a given purpose that can be managed, measured, verified and controlled.

PROCESSING ENGINE: The heart of the IDS, it consists of the instructions (language) for sorting information for relevance, identifying key intrusion evidence, mining databases for attack signatures, and decision-making about thresholds for alerts and initiation of response activities.

PRODUCTION: Software that is being used for a purpose other than when software is being implemented or tested.

PRODUCTION NETWORK: The "production network" is the network used in the daily business of the University of Texas at El Paso. Any network connected to the university backbone, either directly or indirectly, which lacks an intervening firewall device. Any network whose impairment would result in direct loss of functionality to the University of Texas at El Paso employees or impact their ability to do work.

PROFILE: Patterns of a user's activity that can detect changes in normal routines.

PROGRAM: A set of instructions in code that, when executed, causes a computer to perform a task.

PROGRAM POLICY: What management uses to create an organization's security program. It is high-level, comprehensive, and unlikely to need frequent updating.

PROMISCUOUS MODE: Normally an Ethernet interface reads all address information and accepts follow-on packets only destined for itself, but when the interface is in promiscuous mode, it reads all information (sniffer), regardless of its destination.

PROPRIETARY: Belonging to a single company who has legal right and/or ownership of, as a trademark, patent, etc.

PROPRIETARY ENCRYPTION: An algorithm that has not been made public and/or has not withstood public scrutiny. The developer of the algorithm could be a vendor, an individual, or the government.

PROTOCOL: A set of rules for communication between computers. These govern format, timing, sequencing, and error control. These are the rules for communicating. Without these rules, the computer won't make sense of the stream of incoming bits. There can be sets of protocols in some networks, with each protocol handling rules for a subset of the entire task of communication.

PROTOCOL STACK: Related layers of protocol software that function together to implement particular communications architecture.

PROWLER: A daemon that is run periodically to seek out and erase core files, truncate administrative log files, nuke lost+found directories, and otherwise clean up.

PROXY: A firewall mechanism that replaces the IP address of a host on the internal (protected) network with its own IP address for all traffic passing through it. A software agent that acts on behalf of a user, typical proxies accept a connection from a user, make a decision as to whether or not the user or client IP address is permitted to use the proxy, and perhaps does additional authentication. It then completes a connection on behalf of the user to a remote destination.

PROXY SERVER: A server that runs a proxy version of an application, such as e-mail, and filters messages according to a set of rules for that application.

PSEUDO-FLAW: An apparent loophole deliberately implanted in an operating system program as a trap for intruders.

PSTN: Public Switched Telephone Network. Refers to the telephone network or a switching system providing circuit switching to many customers.

PSYCHOLOGICAL OPERATIONS (PSYOP): Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately, the behavior of foreign governments, organizations, groups, and individuals. The purpose of psychological operations is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives.

PUBLIC KEY CRYPTOGRAPHY: Type of cryptography in which the encryption process is publicly available and unprotected, but in which a part of the decryption key is protected so that only a party with knowledge of both parts of the decryption process can decrypt the cipher text. See Asymmetric Key Cryptography.

PUBLIC KEY INFRASTRUCTURE (PKI): A system of certification authorities (CAs) (and, optionally, registration authorities (RAs) and other supporting servers and agents) that perform some set of certificate management, archive management, key management, and token management functions for a community of users in an application of asymmetric cryptography.

PURGE: To render stored applications, files, and other information on a system unrecoverable. See Sanitize.

PURPOSE STATEMENT: The purpose statement explains why the program is being established and what its information security goals are.

PUSH TECHNOLOGY: Technology that allows users to sign up for automatic downloads of online content, such as virus signature file updates, patches, news, and Web site updates, to their e-mail boxes or other designated directories on their computers.

QUANTITATIVE: Have or pertaining to quantity, measurable.

QUANTITATIVE ANALYSIS: Use of formulas to produce a mathematical measure of risk.

READ ACCESS: Permission to read information.

RED BOOK: See Trusted Network Interpretation.

REDUNDANCY: Duplication of system components (e.g., hard drives), information (e.g., backup tapes, archived files), or personnel intended to increase the reliability of service and/or decrease the risk of information loss.

REFERENCE MONITOR: A security control concept in which an abstract machine mediates accesses to objects by subjects. In principle, a reference monitor should be complete (in that it mediates every access), isolated from modification by system entities, and verifiable. A security kernel is an implementation of a reference monitor for a given hardware base.

REFERENCE VALIDATION MECHANISM: An implementation of the reference monitor concept. A security kernel is a type of reference validation mechanism.

RELIABILITY: The probability of a given system performing its mission adequately for a specified period of time under the expected operating conditions.

REMOTE ACCESS: Use of a modem and communications software to connect to a computer network from a distant location via a telephone line or wireless connection.

REMOVE: To remove or clean a virus means to eliminate all traces of it, returning the infected item to its original, uninfected state. Nearly all viruses are theoretically removable by reversing the process by which they infected. However, any virus that damages the item it has infected by destroying one or more bytes is not removable, and the item needs to be deleted and restored from backups in order for the system to be restored to its original, uninfected state. There is a gap between theory and practice. In practice, a removable virus is one that the anti-virus product knows how to remove. The term "clean" is sometimes used for remove, and sometimes used to refer to the destruction of viruses by any method. Thus, deleting a file that is infected might be considered cleaning the system. We do not regard this as an appropriate use of the term "clean."

REPLICATOR: Any program that acts to produce copies of itself. Examples include a program, a worm, a fork bomb, or virus. It is even claimed by some that UNIX and C are the symbiotic halves of an extremely successful replicator.

RESEARCH DATA: Are recorded information, regardless of form in which the information may be recorded, that constitutes the original data that are necessary to support research activities and validate research findings. Research data may include but are not limited to: printed records, observations and notes; electronic data; video and audio records, photographs and negatives, etc.

RESIDENT: A property of most common computer viruses and all background scanners and behavior blockers. A resident virus is one that loads into memory, hooks one or more interrupts, and remains inactive in memory until some trigger event. When the trigger event

occurs, the virus becomes active, either infecting something or causing some other consequence (such as displaying something on the screen). All boot viruses are resident viruses, as are the most common file viruses. Macro viruses are nonresident viruses.

RESIDENT EXTENSION: In PC-DOS, programs can install a part of themselves in memory, and this part can remain active after the program has ended. This memory resident part is called a resident extension, since it is effectively an extension to the operating system. Many viruses install themselves as resident extensions, which will then look for files to infect when those files are accessed or executed later.

RESIDUAL RISK: The potential for the occurrence of an adverse event after adjusting for the impact of all in-place safeguards. See Total Risk, Acceptable Risk, Minimum Level of Protection.

RESIDUE: Data left in storage after processing operations are complete, but before degaussing or rewriting has taken place.

RESOURCE ENCAPSULATION: The process of ensuring that a resource not be directly accessible by a subject, but that it be protected so that the reference monitor can properly mediate accesses to it.

RESTRICTED: The classification of data of which unauthorized disclosure/use would not be in the best interest of an organization and/or its customer's links where users pay for round-the-clock service.

RETROVIRUS: A retrovirus is a virus that waits until all possible backup media are infected too, so that it is not possible to restore the system to an uninfected state.

REVOCATION SYSTEM: A means to prevent use of a certificate.

RISK: A combination of the likelihood that a threat will occur, the likelihood that a threat occurrence will result in an adverse impact, and the severity of the resulting adverse impact. Reducing either the threat or the vulnerability reduces the risk.

RISK ANALYSIS: An analysis of system assets and vulnerabilities to establish an expected loss from certain events based on estimated probabilities of occurrence.

RISK ASSESSMENT: A study of vulnerabilities, threats, likelihood, loss or impact, and theoretical effectiveness of security measures. The process of evaluating threats and vulnerabilities, known and postulated, to determine expected loss and establish the degree of acceptability to system operations.

RISK INDEX: The disparity between the minimum clearance or authorization of system users and the maximum sensitivity (e.g., classification and categories) of data processed by a system. See Risk Management.

RISK MANAGEMENT: The total process of identifying, measuring, and minimizing uncertain events affecting AIS resources. It includes risk analysis, cost benefit analysis, safeguard selection, security test and evaluation, safeguard implementation, and systems review.

RISK-BASED MANAGEMENT: Risk management that considers unquantifiable, speculative events as well as probabilistic events (i.e., uncertainty as well as risk).

ROGUE PROGRAM: This term has been used in the popular press to denote any program intended to damage programs or data, or to breach the security of systems. As such, it encompasses malicious Trojan Horses, logic bombs, viruses, and so on.

ROLES AND RESPONSIBILITIES: Functions performed by someone in a specific situation and obligations to tasks or duties for which that person is accountable. Role-based mapped to job function, assumes that a person will take on different roles, over time, within an organization and different responsibilities in relation to AIS.

ROOTKIT: A hacker security tool that captures passwords and message traffic to and from a computer. A collection of tools that allows a hacker to provide a backdoor into a system, collect information on other systems on the network, mask the fact that the system is compromised, and much more. Rootkit is a classic example of Trojan horse software. Rootkit is available for a wide range of operating systems.

ROUTE: A path through an Internetwork.

ROUTER: An interconnection device that is similar to a bridge but serves packets or frames containing certain protocols. Routers link LANs at the network layer.

ROUTING: The process of choosing the best path to send data (or voice calls) through the network. Routing enables workstations, or nodes, which are not directly connected, to communicate by passing messages along to adjacent nodes.

ROUTING CONTROL: The application of rules during the process of routing so as to choose or avoid specific networks, links, or relays.

RSA ALGORITHM: RSA stands for Rivest-Shamir-Aldeman. A public key cryptographic algorithm that hinges on the assumption that the factoring of the product of two large primes is difficult.

RULES OF BEHAVIOR: The rules that have been established and implemented concerning use of, security in, and acceptable level of risk for the system. Rules will clearly delineate responsibilities and expected behavior of all individuals with access to the system. Rules should cover such matters as work at home, connection to the Internet, use of copyrighted works, unofficial use of government equipment, the assignment and limitation of system privileges, and individual accountability.

RULES-BASED DETECTION: The intrusion detection system detects intrusions by looking for activity that corresponds to known intrusion techniques (signatures) or system vulnerabilities. See Misuse Detection Model.

SAFEGUARD: The logical access controls or the contingency plan in place to mitigate the risk

SAMURAI: A hacker who hires out for legal cracking jobs, snooping for factions in corporate political fights, lawyers pursuing privacy-rights and First Amendment cases, and other parties with legitimate reasons to need an electronic locksmith.

SANITIZE: To expunge data from storage media (e.g., diskettes, CD-ROMs, tapes) so that data recovery is impossible. See Purge.

SATAN: Security Administrator Tool for Analyzing Networks. A tool for remotely probing and identifying the vulnerabilities of systems on IP networks. A powerful freeware program that helps to identify system security weaknesses.

SBU: Sensitive but unclassified.

SCHEDULED CHANGE: Formal notification received, reviewed, and approved by the review process in advance of the change being made.

SCOPE: States which agency resources-hardware, software (operating systems, applications, and communications packages), data, personnel, facilities, and peripheral equipment (including telecommunications)-are to be covered by the security program.

SCREENED HOST: A host on a network behind a screening router. The degree to which a screened host may be accessed depends on the screening rules in the router. See Packet Filtering.

SCREENED SUBNET: A subnet behind a screening router. The degree to which the subnet may be accessed depends on the screening rules in the router. See Packet Filtering.

SCREENING ROUTER: A router configured to perform packet filtering. See Packet Filtering.

SECURE HASH ALGORITHM: Algorithm that can generate a condensed message representation called a message digest.

SECURE NETWORK SERVER: A device that acts as a gateway between a protected enclave and the outside world.

SECURE SHELL: A completely encrypted shell connection between two machines protected by a super long pass-phrase.

SECURITY: A condition that results from the establishment and maintenance of protective measures that ensures a state of inviolability from hostile acts or influences.

SECURITY ADMINISTRATOR: The person charged with monitoring and implementing security controls and procedures for a system. Whereas each agency will have one Information Security Officer, technical management may designate a number of security administrators.

SECURITY ARCHITECTURE: A detailed description of all aspects of the system that relate to security, along with a set of principles to guide the design. Security architecture describes how the system is put together to satisfy the security requirements.

SECURITY AUDIT: A search through a computer system for security problems and vulnerabilities.

SECURITY BASELINE: An established security profile or posture, which has been determined at an established point in time.

SECURITY CONTROLS: Hardware, programs, procedures, policies, and physical safeguards that are put in place to assure the integrity and protection of information and the means of processing it.

SECURITY COUNTERMEASURES: Countermeasures that are aimed at specific threats and vulnerabilities or involve more active techniques as well as activities traditionally perceived as security

SECURITY DOMAINS: The sets of objects that a subject has the ability to access.

SECURITY FAULT ANALYSIS: A security analysis usually performed on hardware at gate level, to determine the security properties of a device when a hardware fault is encountered.

SECURITY FEATURES: The security-relevant functions, mechanisms, and characteristics of AIS hardware and software (e.g., identification, authentication, audit trail, and access control).

SECURITY FILTER: A trusted subsystem that enforces a security policy on the data that passes through it.

SECURITY INCIDENT: In information operations, an assessed event of attempted entry, unauthorized entry, or an information attack on an automated information system. It includes unauthorized probing and browsing; disruption or denial of service; altered or destroyed input, processing, storage, or output of information; or changes to information system hardware, firmware, or software characteristics with or without the users' knowledge, instruction, or intent. Any act or circumstance that involves classified information that deviates from the requirements of governing security publications. For example, compromise, possible compromise, inadvertent disclosure, and deviation.

SECURITY INCIDENT OR BREACH: An event that results in unauthorized, access, loss, disclosure, modification, or destruction of information resources, whether accidental or deliberate.

SECURITY KERNEL: The hardware, firmware, and software elements of a trusted computing base that implement the reference monitor concept. It must mediate all accesses, be protected from modification, and be verifiable as correct.

SECURITY LABEL: Piece of information that represents the sensitivity of a subject or object, such as its hierarchical classification (confidential, secret, top secret) together with any

applicable non-hierarchical security categories (e.g., sensitive compartmented information, critical nuclear weapon design information).

SECURITY LEVEL: The combination of a hierarchical classification and a set of non-hierarchical categories that represents the sensitivity of information.

SECURITY MODE: A mode of operation in which the DAA accredits an AIS to operate. Inherent with each of the four security modes (dedicated, system high, multilevel, and partitioned) are restrictions on the user clearance levels, formal access requirements, need-to-know requirements, and the range of sensitive information permitted on the AIS.

SECURITY OFFICER: The AIS official having the designated responsibility for the security of an AIS system

SECURITY PERIMETER: The boundary where security controls are in effect to protect assets.

SECURITY POLICY: The set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information.

SECURITY POLICY MODEL: A formal presentation of the security policy enforced by the system. It must identify the set of rules and practices that regulate how a system manages, protects, and distributes sensitive information.

SECURITY RANGE: The highest and lowest security levels that are permitted in or on a system, system component, subsystem, or network.

SECURITY REQUIREMENTS: Types and levels of protection necessary for equipment, data, information, applications, and facilities.

SECURITY REQUIREMENTS BASELINE: A description of minimum requirements necessary for a system to maintain an acceptable level of security.

SECURITY RISK: Risks involving platform-specific vulnerabilities.

SECURITY SAFEGUARDS: The protective measures and controls that are prescribed to meet the security requirements specified for an AIS. These safeguards may include, but are not necessarily limited to, hardware and software security features; operation procedures; accountability procedures; access and distribution controls; management constraints; personnel security; and physical structures, areas, and devices.

SECURITY SERVICE: A service, provided by a layer of communicating open systems, which ensures adequate security of the systems or of data transfers.

SECURITY SPECIFICATIONS: A detailed description of the safeguards required to protect a system.

SECURITY STANDARD: A required procedure or management control.

SECURITY TEST AND EVALUATION: An examination and analysis of the security safeguards of a system as they have been applied in an operational environment to determine the security posture of the system.

SECURITY TESTING: A process used to determine that the security features of a system are implemented as designed. This includes hands-on functional testing, penetration testing, and verification.

SECURITY VIOLATION: An instance in which a user or other person circumvents or defeats the controls of a system to obtain unauthorized access to information contained therein or to system resources.

SEGREGATION OF DUTIES: Entails policies, procedures, and an organizational structure established to ensure that no single individual controls all key aspects of physical and/or computer-related operations.

SELF-ENCRYPTING VIRUSES: See Self-Garbling Viruses.

SELF-EXTRACTING FILES: A file that, when run, decompresses part of itself into one or more new files. It is common to store and transmit groups of files in a self-extracting file to conserve both disk space and transmission time. If infected files are compressed into a self-extracting file, anti-virus programs that only scan files will not necessarily be able to detect the virus. To scan such files, you must first extract and then scan their constituent files.

SELF-GARBLING VIRUSES: Some viruses attempt to hide from virus scanning programs by keeping most of their code garbled in some way, and changing the garbling each time they spread. When such a virus runs, a small header degarbles the body of the virus and then branches to it.

SENSITIVE DIGITAL RESEARCH DATA: Are data defined by the University as Category-I data.

SENSITIVITY: The degree to which an AIS system or application requires protection (to ensure confidentiality, integrity, availability), which is determined by an evaluation of the nature and criticality of the data processed, the relation of the system to the organization missions, and the economic value of the system components.

SENSORS: Called probes, monitors, feeds, or taps, they provide information about the system or network targeted for intrusion detection.

SERVER: Any computer providing a service over the network. Services include, but are not limited to: Web site publishing, SSH, chat, printing, wireless access, and file sharing. A computer running a server program is frequently referred to as a server, though it may also be running other client (and server) programs.

SERVICE: A software entity (e.g., process, daemon, or thread) supplying some type of processing upon request.

SESSION STEALING: See IP Splicing.

SHA: Secure Hash Algorithm

SHELL FACILITY: A facility that can be made available for use as a data processing facility in a relatively short period of time with a minimum cost.

SIGNALING SYSTEM 7 (SS-7): A protocol used by phone companies. SS-7 has three basic functions: supervising, alerting, and addressing. Supervising monitors the status of a line or circuit to see if it is busy, idle, or requesting service. Alerting indicates the arrival of an incoming call. Addressing is the transmission of routing and destination signals over the network in the form of dial tone or data pulses.

SIGNATURE: A search pattern, often a simple string of bytes that is expected to be found in every instance of a particular virus. Usually, different viruses have different signatures.

SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP): Software used to control network communications devices using TCP/IP.

SKIPJACK: An NSA-developed encryption algorithm for the Clipper chip. The details of the algorithm are unpublished.

SMURFING: A Denial of Service attack in which an attacker spoofs the source address of an echo-request ICMP (ping) packet to the broadcast address for a network, causing the machines in the network to respond en masse to the victim thereby clogging its network.

SNA: Systems Network Architecture, IBM's proprietary layered communications protocol/architecture.

SNARF: To grab a large document or file for the purpose of using it with or without the author's permission.

SNEAKER: An individual hired to break into places in order to test their security; analogous to tiger team.

SNIFFER: A program to capture data across a computer network. Used by hackers to capture user names and passwords. Software tool that audits and identifies network traffic packets. Is also used legitimately by network operations and maintenance personnel to troubleshoot network problems.

SOCIAL ENGINEERING: An attack based on deceiving users or administrators at the target site. Social engineering attacks are typically carried out by telephoning users, administrators or operators and pretending to be an authorized user, to attempt to gain illicit access to systems. See Incident.

SOFTWARE: The electronically stored commands and instructions that make an AIS functional, including the operating system, applications, and communications protocols.

SOFTWARE SECURITY: General purpose (executive, utility, or software development tools) and applications programs or routines that protect data handled by a system.

SOFTWARE SYSTEM TEST AND EVALUATION PROCESS: A process that plans, develops and documents the quantitative demonstration of the fulfillment of all baseline functional performance, operational and interface requirements.

SOURCE CODE: Refers to the set of commands and instructions making up a program.

SPAM: To crash a program by overrunning a fixed-site buffer with excessively large input data. Also, to cause a person or newsgroup to be flooded with irrelevant or inappropriate messages.

SPECIAL ACCESS PROGRAM: Any program imposing need-to-know or access controls beyond those normally required for access to confidential, secret, or top-secret information. Such a program includes, but is not limited to, special clearance of investigative requirements, special designation of officials authorized to determine need-to-know or special lists of persons determined to have a need-to-know.

SPECIAL TRUST: See POSITION OF SPECIAL TRUST

SPI (SECURE PROFILE INSPECTOR): A network-monitoring tool for UNIX developed by the Department of Energy.

SPLIT-TUNNELING: Simultaneous direct access to a non-University of Texas at El Paso network (such as the Internet, or a home network) from a remote device (PC, PDA, WAP phone, etc.) while connected into the University of Texas at El Paso's network via a VPN tunnel. VPN Virtual Private Network (VPN) is a method for accessing a remote network via "tunneling" through the Internet.

SPOOFING: Unauthorized use of legitimate identification and authentication data, such as user IDs and passwords, by an intruder to impersonate an authorized user or process to gain access to an AIS or data on it.

SPYWARE: Spyware refers to a software program that slips into your computer without your consent to track your online activity. These programs tend to piggyback on another software program. When the user downloads and installs the software, the spyware is also installed without the user's knowledge. There are different forms of spyware that track different types of activity. Some programs monitor what Web sites you visit, while others record key stokes to steal personal information, such as credit card numbers, bank account information or passwords.

SSL (SECURE SOCKET LAYER): A session layer protocol that provides authentication and confidentiality to applications.

STAND-ALONE, SHARED SYSTEM: A system that is physically and electrically isolated from all other systems. It is intended to be used by more than one person; either simultaneously (e.g., a system with multiple terminals) or serially, with data belonging to one

user remaining available to the system while another user is using the system (e.g., a personal computer with non-removable storage media such as a hard disk).

STAND-ALONE, SINGLE-USER SYSTEM: A system that is physically and electrically isolated from all other systems, and is intended to be used by one person at a time, with no data belonging to other users remaining in the system (e.g., a personal computer with removable storage media, such as a floppy disk).

STANDARD: An established rule or model that is measurable; a specific measurement that can be assessed for compliance.

STEALTH VIRUS: A virus that uses any of a variety of techniques to make itself more difficult to detect. A stealth boot virus will typically intercept attempts to view the sector in which it resides, and instead show the viewing program a copy of the sector as it looked prior to infection. An active stealth file virus will typically not reveal any size increase in infected files when you issue the "DIR" command. Stealth viruses must be "active" or running in order to exhibit their stealth qualities.

STORAGE MEDIA: The material on which data are recorded; e.g., paper tape, punched cards, magnetic tape, hard disks, optical disks, etc.

STRONG PASSWORD: A strong password is a password that is not easily guessed. It is normally constructed of a sequence of characters, numbers, and special characters, depending on the capabilities of the operating system. Typically the longer the password the stronger it is. It should never be a name, dictionary word in any language, an acronym, a proper name, a number, or be linked to any personal information about you such as a birth date, social security number, and so on.

SUBNET: A subset of a network's address space used to connect various devices and define message traffic patterns.

SUBVERSION: Occurs when an intruder modifies the operation of the intrusion detector to force false negatives to occur.

SUPERUSER: A user who is authorized to modify and control AIS processes, devices, networks, and file systems.

SUPPORT FOR NONREPUDIATION: The protection of the signing private key (which should never be backed up).

SWITCHED CIRCUITS: Used for traditional phone service where users pay only for the time during which data or voice transmission occurs. In contrast, leased lines are dedicated.

SYMMETRIC CRYPTOSYSTEM: A method of encryption in which the same key is used for both encryption and decryption of the data.

SYMMETRIC KEY CRYPTOGRAPHY: Two or more parties share the same key, which is used both to encrypt and decrypt data.

SYN FLOOD: When the SYN queue is flooded, no new connection can be opened.

SYSTEM: Any device capable of receiving e-mail, browsing web sites, or otherwise capable of receiving, storing, managing, or transmitting data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, PDAs, pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (that is, embedded technology), telecommunication resources, network environments, telephones, fax machines, printers and service bureaus.

SYSTEM ADMINISTRATOR (SA): Person responsible for the effective operation and maintenance of Information Resources, including implementation of standard procedures and controls to enforce the University's security policy.

SYSTEM BOOT RECORDS: Each logical PC-DOS or OS/2 drive (e.g., C:, D:, etc.) has a system boot record associated with it. The system boot record contains code that tells the system about that logical drive and tables that contain an index to the files on it.

SYSTEM CONTROL DATA: Data files such as programs, password files, security tables, authorization tables, etc., which, if not adequately protected, could permit unauthorized access to information resources.

SYSTEM DEVELOPMENT METHODOLOGIES: Methodologies developed through software engineering to manage the complexity of system development. Development methodologies include software engineering aids and high-level design analysis tools.

SYSTEM ENVIRONMENT: The unique technical and operating characteristics of an AIS and its associated environment, including the hardware, software, firmware, communications capability, organization, and physical location.

SYSTEM HIGH SECURITY MODE: A mode of operation wherein all users having access to the AIS possess a security clearance or authorization, but not necessarily a need-to-know, for all data handled by the AIS. If the AIS processes special access information, all users must have formal access approval.

SYSTEM INTEGRITY: Optimal functioning of an AIS, free from unauthorized impairment or manipulation.

SYSTEM INTERCONNECTION: The requirements for communication or interconnection by an AIS with one or more other AIS or networks, to share processing capability or pass data and information in support of multi-organizational or public programs.

SYSTEM MANAGEMENT: Network management functionality embedded in the IDS.

SYSTEM SECURITY OFFICER: Person assigned to implement an organization's computer security policy. Also referred to as a system security program manager. See Security Officer.

SYSTEM SECURITY PLAN: A formal document listing the tasks necessary to meet system security requirements, a schedule for their accomplishments, and to whom responsibilities for each task are assigned.

SYSTEM-SPECIFIC POLICY: The body of rules and practices used to protect a particular information system. System-specific policy is limited to the system or systems affected and may change with changes in the system, its functionality, or its vulnerabilities.

T-1 LINE: A digital carrier facility used to transmit DS-1 formatted digital signals at 1.544 megabits per second. It was the first successful system that supported digitized voice transmission. It is in common use today in Internet service provider (ISP) connections to the Internet

T-3 LINE: A super high-speed connection capable of transmitting data at a rate of 45 million bits per second. This represents a bandwidth equal to about 672 regular voice-grade telephone lines, which is wide enough to transmit full-motion real-time video and very large databases over a busy network. A T3 line is typically installed as a major networking artery for large corporations and universities with high volume network traffic. For example, the backbones of the major Internet service providers are comprised of T3 lines.

TAMPERING: An unauthorized modification that alters the proper functioning of an equipment or system in a manner that degrades the security or functionality it provides.

TANGIBLE: Perceptible by touch.

TASSCC: See Texas Association of State Systems for Computing and Communications.

TCP/IP: Transmission Control Protocol/Internetwork Protocol. The suite of protocols the Internet is based on.

TCP WRAPPER: A software tool for security, which provides additional network logging and restricts service access to authorized hosts by service.

TECHNICAL CONTROLS: Consist of hardware and software controls used to provide automated protection to the system or applications. Technical controls operate within the technical system and applications.

TECHNICAL VULNERABILITY: A hardware, firmware, communication, or software flaw that leaves a computer processing system open for potential exploitation, either externally or internally, thereby resulting in risk for the owner, user, or manager of the system.

TELECOMMUNICATIONS: Preparation, transmission, communication, or related processing of information (text, images, sounds, or other data) by electrical, electromagnetic, or similar means.

TELEPROCESSING: Information handling in which a data processing system uses communications lines. A term for data communications.

TEMPEST: The study and control of spurious electronic signals emitted from AIS equipment.

TERM RULE-BASED SECURITY POLICY: A security policy based on global rules imposed for all users. These rules usually rely on a comparison of the sensitivity of the resources being accessed and the possession of corresponding attributes of users, a group of users, or entities acting on behalf of users.

TERMINAL HIJACKING: Allows an attacker, on a certain machine, to control any terminal session that is in progress. An attack hacker can send and receive terminal I/O while a user is on the terminal.

TERMINAL IDENTIFICATION: The means used to uniquely identify a terminal to a system.

TERMINATE AND STAY RESIDENT: A PC-DOS program that installs a resident extension and then terminates. See Resident Extension.

TEXAS ASSOCIATION OF STATE SYSTEMS FOR COMPUTING AND COMMUNICATIONS (TASSCC): AN independent, self-supporting, and voluntary organization of personnel involved in information resources management within Texas state government.

THREAT: An activity, deliberate or unintentional, with the potential for causing harm to an automated information system or activity.

THREAT AGENT: Methods and things used to exploit vulnerability in an information system, operation, or facility-fire, natural disaster, and so forth.

THREAT ANALYSIS: The examination of all actions and events that might adversely affect a system or operation.

THREAT ASSESSMENT: An evaluation of the nature, likelihood, and consequence of acts or events that could place sensitive information and assets as risk.

THREAT MONITORING: The analysis, assessment, and review of audit trails and other data collected for the purpose of searching out system events that may constitute violations or attempted violations of system security.

TIGER: A software tool that scans for system weaknesses.

TIGER TEAM: Government- and industry-sponsored teams of computer experts who attempt to break down the defenses of computer systems in an effort to uncover, and eventually patch, security holes.

TIME BOMB: A time bomb is a type of logic bomb that is triggered by the arrival of a date or time. See Logic Bomb.

TINKERBELL PROGRAM: A monitoring program used to scan incoming network connections and generate alerts when calls are received from particular sites, or when logins are attempted using certain IDs.

TOPOLOGY: The map or plan of the network. The physical topology describes how the wires or cables are laid out, and the logical or electrical topology describes how the information flows.

TOTAL RISK: The potential for the occurrence of an adverse event if no mitigating action is taken (i.e., the potential for any applicable threat to exploit a system vulnerability). See Acceptable Risk, Residual Risk, Minimum Level of Protection.

TRACE PACKET: In a packet-switching network, a unique packet that causes a report of each stage of its progress to be sent to the network control center from each visited system element.

TRACEROUTE: An operation of sending trace packets for determining information; traces the route of UDP packets for the local host to a remote host. Normally traceroute displays the time and location of the route taken to reach its destination computer.

TRANQUILITY: A security model rule stating that the security level of an active object cannot change during the period of activity.

TRANSACTION: A result-oriented unit of communication processing. One or more commands that are treated as a single unit for the purposes of backup or recovery. Commands within a transaction are committed as a group; i.e., either all of them are committed or all of them are rolled back.

TRANSACTION MANAGEMENT: The activities and functions required in a transaction control process based on a distributed transaction-processing model. This includes ensuring resource managers provide access to shared resources, defining transaction boundaries and specifying actions that constitute a transaction, assigning identifiers to transactions, monitoring the progress of transactions, coordinating multiple resource managers, and managing transaction completion and failure recovery.

TRANSMISSION: The transfer of information over a communications channel.

TRANSMISSION CONTROL PROTOCOL (TCP): A protocol that establishes a connection and provides a reliable transport service between source and destination systems. TCP calls IP to provide a routing service. See Internet Protocol.

TRANSMISSION CONTROL PROTOCOL/INTERNET PROTOCOL (TCP/IP): AN OSI layer 4 (transport) and layer 3 (network) protocol. Used in business for internetworking or combining networks. This network architecture was designed in accordance with standardized concepts.

TRANSPORT LAYER: The fourth layer of the OSI model of data communications. High-level quality control and some alternate routing are done at this level.

TRAP DOOR: Hidden code or hardware device used to circumvent security controls. See Back Door.

TRIPWIRE: A software tool for security. Basically, it works with a database that maintains information about the byte count of files. If the byte count has changed, it will identify it to the system security manager.

TROJAN HORSES: Destructive programs-usually viruses or worms-that are hidden in an attractive or innocent-looking piece of software, such as a game or graphics program. Victims may receive a Trojan horse program by e-mail or on a diskette, often from another unknowing victim, or may be urged to download a file from a Web site or bulletin board.

TRUSTED COMPUTER SYSTEM: (1) An automated information system that employs sufficient hardware and software assurance measures to allow simultaneous processing of a range of classified or sensitive information. (2) A computer system, including all of the hardware, firmware, and software, which, by virtue of having undergone sufficient benchmark validation and testing, as well as acceptance and user testing, can be expected to meet the user's requirements for reliability, security, and operational effectiveness with specified performance characteristics. Such a system is primarily intended for simultaneously processing various levels of sensitive and classified information without danger of compromise.

TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA (TCSEC): A system that employs sufficient hardware and software assurance measures to allow its use for simultaneous processing of a range of sensitive or classified information.

TRUSTED COMPUTING BASE (TCB): The totality of protection mechanisms within a computer system- including hardware, firmware, and software-the combination of which is responsible for enforcing a security policy. A TCB consists of one or more components that together enforce a unified security policy over a product or system. The ability of a TCB to correctly enforce a security policy depends solely on the mechanisms within the TCB and on the correct input by system administrative personnel of parameters (e.g., a user's clearance) related to the security policy.

TRUSTED NETWORK INTERPRETATION: THE specific security features, assurance requirements, and rating structure of the Orange Book as extended to networks of computers ranging from isolated LANs to WANs.

TSR: See Terminate and Stay Resident.

TTY WATCHER: A hacker tool that allows even minimally skilled hackers to hijack terminals. It has a GUI interface.

TUNNELING: A method for circumventing a firewall by hiding a message that would be rejected by the firewall inside a second, acceptable message.

TUNNELING ROUTER: A router or system capable of routing traffic by encrypting it and encapsulating it for transmission across an untrusted network, for eventual de-encapsulation and decryption. See Virtual Network Perimeter.

UNAUTHORIZED DISCLOSURE: The intentional or unintentional revealing of restricted information to people who do not have a legitimate need to access that information.

UNCLASSIFIED: The classification of data that requires no protection against disclosure.

UNIX: Computer operating system originally developed by AT&T. Considered to be very flexible and very powerful. UNIX is capable of multitasking.

UNSCHEDULED CHANGE: Failure to present notification to the formal process in advance of the change being made. Unscheduled changes will only be acceptable in the event of a system failure or the discovery of a security vulnerability.

URL: Universal (or Uniform) Resource Locator; refers to the address of a World Wide Web site.

USER: An individual or automated application that is authorized access to the resource by the owner, in accordance with the owner's procedures and rules.

USER ID: Unique symbol or character string used by an AIS to recognize a specific user.

USER PROFILE: Patterns of a user's activity that can be used to detect changes in normal routines.

USERS: People or processes accessing an AIS either by direct connections (i.e., via terminals) or indirect connections (i.e., prepare input data or receive output that is not reviewed for content or classification by a responsible individual).

UTILITY: A program that performs a specific task for an AIS, such as managing a disk drive or printer.

VACCINES: Program that injects itself into an executable program to perform a signature check and warns if there have been any changes.

VARIANT: A modified version of a virus that is usually produced on purpose by a virus author or by someone who modifies the original virus. Variants may be very similar to their parent virus, or may be fairly different. Some are text variants, which means that the only differences between them and their parent virus are in internal program comments that are never displayed, or in text that is displayed to the screen. Some are the result of small changes made to the original virus, apparently to create a new virus, which is not detected by certain anti-virus programs. Some are the result of large changes, such as combining the spreading part of one virus with the damage part of another.

VENDOR: Someone who exchanges goods or services for money.

VERIFICATION: The process of comparing two levels of system specification for proper correspondence (e.g., security policy model with top-level specification, top-level specification with source code, or source code with object code). This process may or may not be automated.

VIRTUAL NETWORK PERIMETER: A network that appears to be a single protected network behind firewalls, which actually encompasses encrypted virtual links over untrusted networks. Also known as a Virtual Private Network.

VIRTUAL PRIVATE NETWORK: See Virtual Network Perimeter.

VIRUS: A computer program that attaches itself to a file or vulnerable application and delivers a payload that ranges from annoying to extremely destructive without the knowledge or permission of the User. A file virus executes when an infected file is accessed. A macro virus infects the executable code embedded in Microsoft Office programs that allow users to generate macros.

VIRUS SIGNATURE: Alterations to files or applications indicating the presence of a virus, detectable by virus scanning software.

VULNERABILITY: A weakness that may be exploited by a threat agent to cause harm to the AIS. The totality of susceptibilities to specific attack and the opportunity available to a hostile entity to mount that attack.

VULNERABILITY ANALYSIS: Systematic examination of an AIS or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

VULNERABILITY ASSESSMENT: An examination of the ability of a system or application, including current security procedures and controls, to withstand assault. A vulnerability assessment may be used to (1) identify weaknesses that could be exploited and (2) predict the effectiveness of additional security measures in protecting information resources from attack.

VULNERABILITY AUDIT: The process of identifying and documenting specific vulnerabilities in critical information systems.

VULNERABILITY SCANNERS: Perform rigorous examinations of systems to identify weaknesses that might allow security violations.

Vx: This term is shorthand for Virus Exchange. It is most often applied to electronic bulletin board systems where viruses are made available for download (a VxBBS).

WAIS (WIDE AREA INFORMATION SERVICE): An Internet service that allows you to search a large number of specially indexed databases.

WAN: Wide Area Network.

WAR DIALER: A program that dials a given list or range of numbers and records those which answer with handshake tones that might be entry points to computer or telecommunications systems.

WEB PAGE: A document on the World Wide Web. Every Web page is identified by a unique URL (Uniform Resource Locator).

WEB SERVER: A computer that delivers (serves up) web pages.

WEB SITE: A location on the World Wide Web, accessed by typing its address (URL) into a Web browser. A Web site always includes a home page and may contain additional documents or pages. See World Wide Web.

WHOM PERSON: One who practices within an area of expertise.

WIDE AREA NETWORK (WAN): A data communications network designed to serve an arm of hundreds or thousands of miles. WANs can be a public or private network using packet switching or the circuit switched telephone network.

WORK-AROUND: A temporary method of fixing or getting around the problem.

WORLD WIDE WEB (WWW): A system of Internet hosts that supports documents formatted in HTML (Hypertext Markup Language) that contain links to other documents (hyperlinks) and to audio, video, and graphic images. Users can access the Web with special applications called browsers, such as Netscape, Navigator, and Microsoft Internet Explorer.

WORM: A program that makes copies of itself elsewhere in a computing system. These copies may be created on the same computer or may be sent over networks to other computers. The first use of the term described a program that copied itself benignly around a network, using otherwise-unused resources on networked machines to perform distributed computation. Some worms are security threats, using networks to spread themselves against the wishes of the system owners and disrupting networks by overloading them. Similar to a virus in that it makes copies of itself, but different in that it need not attach to particular files or sectors at all.

WRITE: A fundamental operation that results only in the flow of information from a subject to an object.

WRITE ACCESS: Permission to write to an object.

WWW: See World Wide Web.

ZIP FILES: Files compressed with the PKZIP compression program. PKZIP is a popular compression program. Many virus scanners today, including IBM Antivirus, can scan inside ZIP files. See Self-Extracting Files.

ZOO VIRUS: A virus rarely reported anywhere in the world, but exists in the collections of researchers. A zoo virus has some "escaping" virus collections, and infecting user machines. Its prevalence could increase to the point that it is considered "in the wild."

Revision History
First Draft: December 24, 2001
Revised: January 10, 2002
Revised: March 27, 2002
Revised: September 17, 2002
Revised: September 19, 2002
Revised: January 23, 2012