

Information Resources Security Operations Manual

April 3, 2008

Office of Technology and Information Services
The University of Texas System Administration

Table of Contents

1. Overview.....	2
2. Acceptable Use.....	2
3. Account Management	2
4. Administrative/Special Access	2
5. Backup of Network Servers.....	3
6. Change Management	3
7. Computer Virus Prevention.....	4
8. Classification of Sensitive Digital Data	4
9. Risk Management	4
10. Reduction of Use and Collection of Social Security Numbers	5
11. Management of Sensitive Digital Data	5
12. Email	5
13. Incident Management.....	6
14. Internet Use.....	6
15. Information Services (IS) Privacy	7
16. Network Access.....	7
17. Network Configuration.....	7
18. Passwords.....	8
19. Physical Access:	9
20. Portable Computing and Remote Access.....	9
21. Security Monitoring.....	10
22. Security Training	11
23. Server and Network Device Hardening Standards	11
24. Software Licensing.....	12
25. Project Management Guidelines	12
26. System Deployment	12
27. Vendor and Contract Employee Access	12
28. Right to Monitor	14
29. Disciplinary Actions	14
30. Removal, Re-Deployment, and Disposal of Equipment and Media.....	14
31. Incidental Use	16
32. Sharing Documents with External Entities	16
APPENDIX 1 - DEFINITIONS.....	17
APPENDIX 2 – STRONG PASSWORD GUIDELINES.....	21
APPENDIX 3 - ENCRYPTION GUIDELINES.....	24
APPENDIX 4 – MINIMUM STANDARDS FOR PORTABLE COMPUTING	26
APPENDIX 5 – QUALITY ASSURANCE GUIDELINES – PROJECT MANAGEMENT REQUIREMENTS	27
NOTE: MODEL GUIDELINES POSTED AT WWW.DIR.STATE.TX.US/EOD/QA SHOULD BE USED	
APPENDIX 6 – SAMPLE MEMORANDUM OF UNDERSTANDING.....	28
APPENDIX 6 – SAMPLE MEMORANDUM OF UNDERSTANDING.....	29

1. Overview

The Information Resources Security Operations Manual provides guidance and defines procedures relating to the operational implementation of the UTS165 - U.T. System-wide Administration Information Resources Use and Security Policy and the INT124 U.T. System Administration Information Resources Acceptable Use and Security Policy. These three documents comprise the whole of the policy and procedures foundation for computer security at U.T. System Administration which for purposes of this document shall be referred to as the **Computer Policies and Procedures**.

The U.T. System Administration Information Security Operations Manual provides guidance for all individuals that have, or may require, access to U.T. System Administration Information Resources and those with responsibility for maintaining the Information Resources at U.T. System Administration.

2. Acceptable Use

Before an individual is given access to a U.T. System Administration system resource he or she must sign the Information Resources Acceptable Use Policy Acknowledgement form.

3. Account Management

Proper management and use of computer accounts are basic requirements for protecting U.T. System Administration Information Resources. All account passwords, including default passwords, are to be constructed and managed in accordance with the Computer Policies and Procedures. The following account management practices apply:

- All accounts for access to the U.T. System Administration network must have an associated Network Request Form that includes approval by the Owner of the information for the assigned access to information resources for the position and duties of the individual. This includes accounts created for use by outside vendors and contract employees (see section entitled Vendor and Contract Employee Access).
- Each new User signs the U.T. System Administration User Acknowledgement agreement which is part of the Acceptable Use Policy before access is given to the User's account.
- All accounts are uniquely identifiable by an assigned user name.
- All vendor accounts are required to have a password expiration date.
- Accounts of individuals on extended leave (more than 30 days) or accounts that have not been accessed within 30 days are disabled.
- Accounts of individuals who have changed roles within U.T. System Administration or who have separated from their relationship with U.T. System Administration will be changed to reflect current needs, removed or disabled.
- Existing accounts are reviewed at least on a quarterly basis and unused accounts are disabled.
- Disabled accounts are reviewed at least on a quarterly basis to determine if the accounts and associated directories, if any, can be removed.

4. Administrative/Special Access

All users of administrative/special access accounts must be made aware of special responsibilities associated with the use of special access privileges and not abuse such privilege. All persons with administrative, special access must adhere to the following access requirements.

- Individuals that use administrative/special access accounts must use these accounts only for their intended administrative purposes. They may perform investigations relating to potential misuse of Information Resources by an individual User only under the direction of the Information Security Officer, Chief Information Officer or executive management.

- Each account used for administrative/special access must adhere to the U.T. System Administration password requirements.
- U.T. System Administration departments must submit to the Office of Technology and Information Services a list of administrative contacts for any systems connected to and applications running on the U.T. System Administration network.
- All Information Technology Professionals acting as custodians of U.T. System Administration data will sign a Memorandum of Understanding relating to their custodial role and responsibilities. See Appendix 6 for sample form.
- The password for a shared administrator/special access account must change when any individual knowing the password leaves the department or U.T. System Administration, or changes role, or upon a change in the vendor personnel assigned to U.T. System Administration contracts.
- For each secured system there must be a password escrow procedure in place to enable someone other than the administrator to gain access to the system in an emergency situation. Individual user passwords are not escrowed.
- When special access accounts are needed for auditing, software development, software installation, or other defined need, they:
 - Must be authorized by the Information Security Officer
 - Must be created with an expiration date.
 - Must be removed when work is complete.

5. Backup of Network Servers

Electronic backups are a business requirement to enable the recovery of data and applications in the case of events such as natural disasters, system disk drive failures, espionage, data entry errors, human error, or system operations errors. The U.T. System Administration uses the following backup practices:

- All U.T. System Administration servers containing data or programs are backed up as determined by the data owner, in consultation with technical staff. The backup and recovery plan must incorporate disasters, hardware failures, espionage, data errors, human errors or system operations errors.
- The Office of Technology and Information Services is the department with operational responsibility for backup of all servers connected to the U.T. System Administration network.
- The Office of Technology and Information Services maintains a backup and recovery plan that includes the following:
 - Requirements for off site storage and vendors.
 - Physical access controls for onsite and offsite storage and media in transit.
 - Processes to ensure backups are viable and can be recovered.
- The System Audit Office periodically reviews the backup and recovery plan.

6. Change Management

The Information Resources infrastructure at U.T. System Administration is constantly changing and evolving to support the missions of the organization and its many departments. Computer networks, servers, and applications require planned outages for upgrades, maintenance, and fine-tuning. To ensure reliable and stable operations, change logs are maintained to assist with problem resolution. The following change management procedures apply:

- All changes affecting computing environmental facilities (e.g., air-conditioning, water, heat, plumbing, electricity, and alarms) should be coordinated with and reported to the Manager of Information Technology Support or the Information Resources Manager.
- The Office of Technology and Information Services management may deny a scheduled or unscheduled change for reasons including, but not limited to, inadequate planning, inadequate back out contingencies, inopportune timing in terms of impact on service to Users or in relation to

key business processes such as year end accounting, or lack of resources to address potential problems that may be caused by the change.

- Whenever possible customers will be notified for scheduled and unscheduled changes following the steps contained in the Network Change Management Procedures in the Office of Technology and Information Services Procedures, guidelines and Standards document.
- Each change is subject to review and is the responsibility of the Information Technology leader in that area whether scheduled or unscheduled. The Office of Technology and Information Services can opt into review of a change process.
- The Office of Technology and Information Services maintains a Change Management Log for all significant changes, including emergency changes. Change management procedures for all emergency and non-emergency changes must be maintained. At a minimum, log entries are to contain the following:
 - Identify, classify and prioritize the change
 - Assess the impact of the change
 - Date of submission and date of change
 - Owner and custodian contact information who authorized the change
 - Notation of testing of the change
 - Implementation plan and back-out plan for the change
 - Indication of success or failure
 - Documentation and tracking of change

7. Computer Virus Prevention

A variety of technologies and practices are required to protect the U.T. System Administration network infrastructure and other Information Resources from threats posed by computer viruses, worms, and other types of hostile computer programs.

- The Office of Technology and Information Services must install current virus protection software on all U.T. System Administration computers on the U.T. System Administration network.
- Virus protection software installed on U.T. System Administration computers will automatically be registered with the anti virus server.
- Email gateways must utilize properly maintained email virus protection software.
- Any computer identified as a security risk due to lack of virus protection or other risk factor may be disconnected from the network and the account disabled until adequate protection is in place.
- Every instance of a computer virus infection constitutes a security incident and must be reported to the Office of Technology and Information Services Help Desk. When required the Office of Technology and Information Services will initiate the Virus Response Plan.

8. Classification of Sensitive Digital Data

Owners of Information Resources shall classify all digital assets based on confidentiality, sensitivity and risk. Sensitive data identified must comply with state and federal regulation, but may exceed these standards.

9. Risk Management

Responsibility for risk assessment is divided between the Data Owners, the Data Custodians and the Office of Technology and Information Services. Each has responsibility for those parts of risk management in their control.

- An annual Information Resources Security Risk Assessment will be procured by the Office of Technology and Information Services for all technologies on the U.T. System Administration network.

- Data Owners and Data Custodians are responsible for the risk assessment their organizations in the handling of confidential and sensitive data in their control and compliance with state and federal guidelines.

10. Reduction of Use and Collection of Social Security Numbers

Each individual who access the U.T. System Administration Information Resources must comply will all policies concerning the control of Social Security Numbers and other sensitive personal data.

- New systems or major changes to existing systems must be reviewed by the Information Security Officer for compliance with Social Security Number regulations prior to purchase or during design.
- Only Employee Benefits, Employee Services, Police Department (for the Cadet Academy) and Risk Management are authorized to collect SSNs
- The Office of Technology and Information Services shall issue a unique identifier for each individual accessing Information Resources or references by systems managed by U.T. System Administration.

11. Management of Sensitive Digital Data

The appropriate control of sensitive digital data is the responsibility of every U.T. System Administration employee or vendor contracted to manage sensitive data. They must be cautious in their use of sensitive information and make prudent decisions in the release of the information to any other person or company.

- The Office of Technology and Information Services has responsibility for management and monitoring access to sensitive data on the U.T. System Administration network.
- Data Owners and Data Custodians have responsibility for management and monitoring access to sensitive data off the U.T. System Administration network.
- Access control lists to sensitive data must be reviewed quarterly by the data Owner or service provider.
- Access to U.T. System Administration Information Resources equipment spaces must be logged and monitored.
- The Office of Technology and Information Services has responsibility for the security plan for U.T. System Administration.
- All workstations owned by U.T. System Administration must use encryption software.
- All sensitive data in transit must be encrypted

12. Email

Email is an essential tool for communicating within the University of Texas System. It is important that unimpeded email services be available at all times and that email be used in a manner that achieves its purpose without exposing U.T. System Administration to unnecessary technical, financial, or legal risks. The following practices apply:

- Mailbox size is determined by availability of storage resources and business need. The Information Resource Manager or his designee must approve an increase in an employee's or his/her designee's mailbox size based on business need and prudent use of resources. The approval process includes an analysis of the mailbox (review of message subject lines) to determine the business need for increase.
- All User activity on U.T. System Administration Information Resources assets is subject to logging and review.
- Business related email should not be forwarded to other email accounts.
- To reduce spam and protect the email environment from malicious virus, worm or other threat the Office of Technology and Information Services may filter block and/or strip potentially harmful code from messages originating from sites known for distribution of spam or malicious code.

13. Incident Management

Incident management is needed to protect U.T. System Administration Information Resources and assure continued operations in the event of a security breach or incident involving computer virus, worm, attack against university information systems, or misuse of Information Resources. The Office of Technology and Information Services is required to establish and follow Incident Management Procedures to ensure that each incident is reported, documented and resolved in a manner that restores operation quickly and if required, maintains evidence for further action and possible review by law enforcement.

The following standard operating procedure applies:

- U.T. System Administration employees must report all security incidents to either their supervisor, department head, Information Security Officer or the Office of Technology and Information Services Help Desk.
- U.T. System Administration will have a Computer Incident Response Team organized by the Information Security Officer that in the event of a computer security incident will initiate and follow the Incident Management Procedures. The members of this team will have predefined roles and responsibilities which, based on the severity of the incident, may take priority over normal duties.
- Whenever a security incident such as a virus, worm, hoax email, hacker attack, Trojan horse, etc. is suspected or confirmed, Incident Management Procedures will be followed.
- The Information Security Officer is responsible for reporting the incident to:
 - U.T. System executive management.
 - Computer Incident Response Team
 - The Texas Department of Information Resources as outlined in TAC 202.7(f).
 - The U.T. System Administration Office of the Director of Police.
 - The Office of Human Resources.
- The Information Security Officer will determine if a widespread U.T. System Administration communication is required, the content of any such communication, and the method of distribution. U.T. System Executive Officers, the CISO and/or the Office of Public Affairs will handle any communications to the general public.
- The Office of Technology and Information Services will present the chain of evidence to the Office of the Director of Police and/or the Office of Human Resources to determine if outside law enforcement must be notified.
- The Information Security Officer is responsible for determining the physical and electronic evidence to be gathered as part of the incident investigation, except in cases involving appropriate law enforcement personnel, where they will make these determinations.
- Technical staff from the Computer Incident Response Team led by the Information Security Officer is responsible for ensuring that any damage from a security incident is repaired or mitigated and that the vulnerability is eliminated or minimized.
- The Information Security Officer is responsible for communicating new issues or vulnerabilities to vendor(s) as needed, and for working with the vendor(s) to eliminate or mitigate the vulnerabilities.
- The Information Security Officer is responsible for initiating, completing, and documenting the incident investigation with assistance from the Computer Incident Response Team
- The U.T. System Office of the Director of Police serves as liaison with law enforcement organizations.

14. Internet Use

U.T. System Administration network Users must adhere to prudent and responsible Internet practices to mitigate risks associated with the Internet. The following practices apply:

- The Office of Technology and Information Services makes every effort to ensure that software used to access the Internet incorporates appropriate security features and patches and does not expose U.T. System Administration Information Resources to unnecessary security risks.
- Content on all U.T. System Administration web sites must be business related and must be approved by the U.T. System Administration department publishing the information.

- Purchases handled via the Internet are subject to the U.T. System Administration procurement rules.
- Personal commercial advertising must not be posted on U.T. System Administration web sites.
- U.T. System Administration data may be made available via U.T. System Administration web sites only by those groups and individuals who are duly authorized.
- All confidential, personally identifiable, protected health information or student data transmitted over the Internet must be encrypted in accordance with Encryption Guidelines (see Appendix 3)

15. Information Services (IS) Privacy

To manage systems and enforce security, U.T. System Administration may log, review, and otherwise utilize any information stored on or passing through its Information Resource systems in accordance with the provisions and safeguards provided in the Texas Administrative Code 202.1-8, Information Resource Standards.

In suspected cases of abuse of Information Resources, the contents of any email or file may be reviewed in accordance with provisions defined in the Disciplinary section of the Information Resources Information Use and Security Policy.

Access to data will be limited in scope based on business need.

16. Network Access

Access to the network is managed to ensure the reliability of the network and the integrity and appropriate use of information contained within the network: The following network access procedures apply:

- Only network addresses issued by the U.T. System Administration Office of Technology and Information Services may be used on the U.T. System Administration network except as noted below.
- No network hardware (router, switch, hub, firewall, wireless access point, or other network appliance) may be installed on the U.T. System Administration network without approval from the Office of Technology and Information Services.
- To ensure that systems meet minimal acceptable guidelines for compatibility and security, The Office of Technology and Information Services must approve any non U.T. System Administration owned computer systems that attach to the U.T. System Administration network. Requirements are:
 - Granting of administrative privileges on equipment to U.T. System Administration Information Security Staff
 - Installation of and automated updates of Symantec Antivirus
 - This should be initially installed from a thumb drive and the hard drive scanned prior to connecting the computer to the network.
 - Installation of and periodic updates by Spysweeper
 - Installation of and regular updates from Hercules
 - Regular connection to the UT System Administration domain to acquire appropriate security patches.

To ensure compatibility with the U.T. System Administration network, all computers, PDA's and office productivity software purchased by the U.T. System Administration must adhere to standards established by and be approved by the Office of Technology and Information Services.

17. Network Configuration

The U.T. System Administration manages the network infrastructure, which includes all cabling and connected electronic devices, to ensure reliability of operations, proper accessibility to resources, and protection of data confidentiality and integrity.

The Office of Technology and Information Services

- Maintains a reliable network with as much built-in redundancy as is feasible to acquire and maintain.
- Maintains all network servers.
- Installs or authorizes a contractor to install all cabling and network hardware.
- Approves the specification used to configure all equipment connected to the U.T. System Administration network.
- Makes all changes to the configuration of active network management devices.
- Sets all protocols and standards used on the U.T. System Administration network.
- Manages all connections of the network infrastructure to external third party networks. This includes connections to external telephone networks.
- Installs and maintains U.T. System Administration network firewalls configured following the U.T. System Administration Firewall Implementation Standard documentation.
- Provides written authorization for the use of departmental firewalls. Their use is not permitted without the written authorization.

Limitations to the Network devices include:

- No hub devices may be connected to the network as they obscure individual devices on the network.
- Devices of any kind which are not the property of U.T. System Administration or are not managed by the Office of Technology and Information Services may not connect to the network.

18. Passwords

Strong passwords are required on U.T. System Administration network accounts. All passwords, including initial passwords, must be constructed, implemented, and maintained according to the following:

- Passwords must:
 - Be changed at least annually.
 - Be changed immediately if the security of the password is in doubt.
 - Be treated as confidential information.
 - Have a minimum length of 8 characters.
 - Be comprised of a combination of alpha, numeric, or special characters of which at least one character is alpha and one is numeric.
 - Be encrypted when stored or transmitted.
- Passwords must not:
 - Be reused within one year after expiration.
 - Be shared with anyone except as necessary for systems maintenance, and in such case must immediately be changed after completion of the maintenance.
 - Be constructed from information easily related to the account owner such as: user name, logon ID, given name, social security number, nickname, telephone number, relative's names, birth date, etc.
 - Be dictionary words (English or foreign), acronyms, or popular phrases.
 - Be the same as passwords selected for personal use such as passwords commonly used on public web sites.
- Security tokens may only be issued by the Office of Technology and Information Services (i.e. Smartcards and other access and identification devices). These devices must be returned on demand or upon termination of the relationship with U.T. System Administration.
- All systems should be configured to allow Users to change their own passwords upon demand without third-party involvement.
- Administrators must not circumvent the password guidelines requirements for the sake of ease of use.
- Unattended computing devices must be secured from unauthorized access. Physical security options include barriers such as locked doors or security cables. Logical security options include screen saver passwords and automatic session time-outs.

- The Office of Technology and Information Services Helpdesk password change procedures must include the following:
 - Authentication of the User prior to changing the password (*Acceptable forms of authentication include recognition of the User's voice on the telephone, having the User come to the helpdesk with identification to request the password change, or accepting the request from a department contact who has verified that the user requires a password change*).
 - Changing to a strong password.
 - Requiring the User to change the password at first login.

For more information on creating secure "strong" passwords please see the Password Guidelines published by the Office of Technology and Information Services (Appendix 2).

19. Physical Access:

The granting, controlling, and monitoring of physical access is an important component of the overall security program:

- Physical access to all Information Resources restricted facilities must be managed.
- All Information Resource facilities must be physically protected in proportion to the criticality or importance of their function at U.T. System Administration, and the confidentiality of any impacted data resources affected.
- Access to Information Resources facilities must be granted only to U.T. System Administration personnel and contractors whose job responsibilities require access to that facility.
- The process for granting access to Information Resource facilities must include the approval of the Information Resource Manager or designee or his or her designee.
- Access cards and/or Information Resource areas keys must not be shared or loaned to others.
- Access cards, and/or keys, and badges that are no longer required must be returned to the Office of Human Resources, Business and Administrative Services or the Office of the Director of Police. All returned access cards must be forwarded to the Office of the Director of Police (ODOP) as soon as possible. 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 Office of Director of Police as soon as possible.
- The U.T. System Administration Office of the Director of Police maintains card access records and visitor logs for Information Resources facilities.
- The person responsible for the Information Resources facility must notify the Office of Director of Police as soon as possible to remove the card and/or key access rights of individuals that change roles within the U.T. System Administration or who are separated from their relationship with U.T. System Administration.
- Visitors must be escorted in controlled areas of Information Resources facilities.
- The Information Resource Manager or a designee must review access records for secured Information Resource facilities on a periodic basis and investigate any unusual access.
- The Information Resource Manager or a designee must review card and/or key access rights for secured Information Resource facilities on a periodic basis and remove access for individuals that no longer require access.
- Signage for restricted access rooms and locations must be practical. Minimal discernible evidence of the importance of the location should be displayed.

20. Portable Computing and Remote Access

Computers and devices used to access the U.T. System Administration infrastructure must do so in a manner that preserves the integrity, availability, and confidentiality of U.T. System Administration information.

- Remote access to the U.T. System Administration network may be made only through approved connection methods (i.e. modem pool, VPN, Terminal Services, or approved wireless protocols). All remote Users must comply with the Minimum Standards for Portable Computing (see Appendix 4). Computers not managed by U.T. System Administration staff may only connect to the U.T. System Administration network and Information Resources via Terminal Services and/or use Web mail.
- Computers managed by U.T. System Administration staff must connect to the U.T. System Administration network and Information Resources via VPN.

21. Security Monitoring

Security monitoring is used to confirm that security practices and controls in place are being adhered to and are effective. Monitoring consists of activities such as automated notification of security breaches and automated or manual review of logs and error files. The following monitoring requirements apply to Information Resources at U.T. System Administration and are the responsibility of the Office of Technology and Information Services.

- Based on risk assessment, operating system, user accounting, and application software audit logging processes will be enabled on host and server systems
- Login attempt monitoring, reporting, and automated lockout after three failed attempts must be enabled
- 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 systems must be enabled.
- Automated tools will provide real time notification of detected wrongdoing and vulnerability exploitation. Where possible a security baseline will be developed and the tools will report exceptions to the extent technically feasible. These tools will be deployed to monitor:
 - Internet traffic
 - Electronic mail traffic
 - Local Area Network traffic, protocols, and device inventory
 - Operating system security parameters
 - Disk utilization
- The following files will be monitored for signs of wrongdoing and vulnerability exploitation at a frequency determined by risk:
 - Server logs
 - Automated intrusion detection system logs
 - Firewall logs
 - User account logs
 - Network scanning logs
 - System error logs
 - Application logs
 - Data backup and recovery logs
 - Help desk trouble tickets
 - Failed Login report
 - Telephone activity - Call Detail Reports
- The following checks will be performed at least annually by assigned individuals:
 - Password strength
 - Unauthorized network devices
 - Unauthorized network servers
 - Unauthorized personal web servers
 - Unauthorized modem use
 - Operating System and Software Licenses Inventory
- Any security issues discovered will be reported to the Information Security Officer and appropriate executive officials (see Disciplinary Actions section of this manual).

22. Security Training

The Office of Technology and Information Services is charged with providing a combination of general computer security awareness and supported products training. Training responsibilities includes:

- Preparation, maintenance, and distribution of information that concisely describes U.T. System Administration Information security policies and procedures.
- Development and maintenance of a process to communicate new computer security program information, security bulletin information, and security items of interest to employees.
- Provision of specific security training to Information Technology Professionals serving in positions of special trust (for example, system administrators).

Individual Training responsibilities

New Employees

- All new Users will receive introductory security awareness training at new employee orientation.

All Employees:

- All Users of U.T. System Administration Information Resources will be provided with training and supporting reference materials to allow them to properly protect U.T. System Administration Information Resources.
- All users must sign an acknowledgement stating they received the information about U.T. System Administration requirements regarding computer security policies and procedures (part of the Acceptable Use Policy).

Information Technology Professionals

- All IT Professionals must take 3 hours of security training relevant to their responsibilities annually.

23. Server and Network Device Hardening Standards

Servers are used to deliver information and services throughout U.T. System Administration. Information and services must be delivered securely and reliably to assure that data integrity, confidentiality, and availability are preserved. To achieve these goals, servers must be installed and maintained in a manner that minimizes service disruptions and prevents unauthorized access or use. The following standards apply:

- A server must not be connected to the U.T. System Administration network until it is in a secured state and location (as determined by the Network Security Officer).
- All server installations must follow the Server Hardening Procedure that provides detailed information required to harden a server. The following general steps are included in the Server Hardening Procedure:
 - Installation of the operating system from a reliable source.
 - Application of vendor supplied patches.
 - Removal of unnecessary software, system services, and drivers.
 - Setting of security parameters, file protections and enabling of audit logging.
 - Disabling or changing of passwords associated with default accounts.
 - Installation of appropriate intrusion detection and/or file integrity software.
- To ensure compatibility in the U.T. System Administration computing environment, OTIS must specify, configure, install and maintain all servers.
- The OTIS monitors security issues, both internal and external to U.T. System Administration and manages the installation of security patches on behalf of U.T. System Administration.
- The OTIS tests security patches before installation where technically feasible.
- The OTIS may make hardware resources available for testing security patches for special applications.

- The OTIS must implement Security patches in a timely manner.
- The OTIS scans all servers on a monthly basis to verify that necessary patches have been installed.

24. Software Licensing

To ensure that all software used on U.T. System Administration computers will be used in accordance with the applicable software license:

- U.T. System Administration will provide a sufficient number of licensed copies of software to enable employees to perform their work in an expedient and effective manner. Management must make arrangements for additional licensed copies if additional copies are needed.
- Only software approved for use by the Office of Technology and Information Services may be installed on System Administration computers.
- Systems administrators have the right to remove software from U.T. System Administration computers for cause. For example, if User can't show proof of license, or if the software is not required for business purposes, or causes problems on the System owned computer.
- The Office of Technology and Information Services will run periodic scans of network computers to inventory installed software.
- U.T. System Administration 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.

25. Project Management Guidelines

The protection of Information Resources (including data confidentiality, integrity, and accessibility) must be considered during the development or purchase of new computer applications.

- The Office of Technology and Information Services is responsible for developing, maintaining, and providing leadership in project management practices as appropriate for projects of varying scope, cost, and risk. All software developed in-house which runs on production systems must follow the Office of Technology and Information Services Project Management Guidelines (see Appendix 5), which incorporate security of the system.

26. System Deployment

- Development of software should enforce source control.
- Separate production and development environments will be maintained to ensure the security and reliability of the production system. Exceptions to this must be approved by the Information Resources Manager.
- Deployment must adhere to Change Management requirements (see Section 6)
- Deployment must follow standard community guidelines for communication of changes.

27. Vendor and Contract Employee Access

Vendors serve an important function in the support of hardware and software and in some cases possibly even the operations of computer networks, servers, and/or applications.

- Vendors must comply with the Information Resources Use and Security Policy, and any U.T. System Administration department engaging a vendor must provide the vendor with a copy of this policy and any other procedures they must follow, including, but not limited to:
 - Safety
 - Privacy
 - Security
 - Auditing
 - Software licensing

- Acceptable Use
- Vendors will adhere to Federal and State laws to which U.T. System Administration must adhere.
- Vendor agreements and contracts must specifically reference U.T. System-wide The Information Resources Use and Security Policy, the U.T. System Administration Information Resources Acceptable Use and Security Policy, and the Information Resources Security Operations Manual.
- Vendor agreements and contracts must address the following issues:
 - the U.T. System Administration information the vendor may access.
 - the vendor's responsibility to protect U.T. System Administration information.
 - the vendor's responsibility regarding the deletion, destruction, disposal or return of U.T. System Administration information at the end of the contract.
 - the vendor's responsibility to use U.T. System Administration information only for the purpose of the business agreement.
 - U.T. System Administration's right to audit and otherwise verify the security of university information and other resources in the possession of or being managed by the vendor and the University's right to investigate any security breaches involving these resources.
- The U.T. System Administration will provide an Information Resources 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 U.T. System Administration with a list of all employees working on the contract. The list must be updated and provided to U.T. System Administration within 24 hours of staff changes.
- The Owner of the information has the right to approve or disapprove for cause any vendor employee having access to U.T. System Administration sensitive or confidential information.
- Vendors must report all security incidents to the U.T. System Administration Information Resource Manager or Information Security Officer.
- Each vendor must follow all applicable U.T. System Administration change control processes and procedures approved by the Office of Technology and Information Services.
- For contracts involving onsite work, regular work hours and duties will be defined in the contract. The Information Resource Manager and the department head of the department receiving the contract work must approve in writing work outside defined parameters.
- All vendor accounts and maintenance equipment connecting the U.T. System Administration network to the Internet or outside organizations will remain disabled except when in use for authorized maintenance.
- Vendor accounts providing access to U.T. System Administration Information Resources must be uniquely identifiable and passwords must comply with the U.T. System Administration password requirements as detailed in this manual.
- Vendors and Contract Employees wishing to use non-UT System computers on the UT System network must comply with Network Access standards outlined in Section 16.
- Vendors must maintain a log of major work activities that is available to U.T. System Administration management upon request. Logs may include such events as personnel changes, password changes, project milestones, deliverables, and arrival and departure times, as necessary for a given contract.
- For contracts involving offsite work, vendor remote access to the U.T. System Administration network may be made available only after written approval by the Office of Technology and Information Services and through Terminal Services.
- Upon departure of a vendor employee from a U.T. System Administration contract for any reason, the vendor will ensure that the employee's access to all U.T. System Administration sensitive and confidential information is removed within 24 hours in a manner agreed upon by U.T. System Administration.
- Upon termination of a contract or at the request of U.T. System Administration, the vendor will return, delete or destroy all U.T. System Administration information and provide written certification of that return, deletion, or destruction within 24 hours.
- Upon termination of a contract or at the request of U.T. System Administration, the vendor must immediately surrender all U.T. System Administration property and Information Resources.

Authorized U.T. System Administration management must document any equipment and/or supplies to be retained by the vendor.

- Vendors are required to comply with all State of Texas and U.T. System Administration auditing requirements, including the auditing of the vendor's work.
- All software used by the vendor in providing service to U.T. System Administration must be properly inventoried and licensed. Software provided by U.T. System Administration installed on vendor equipment must be removed at the end of the contract.
- All vendor accounts are required to have an expiration date.
- To protect the University of Texas System intellectual property information technology vendor contracts must be in accordance with the Board of Regents' Rules and Regulations concerning intellectual property available on the System Administration web site.

28. Right to Monitor

The Office of Technology and Information Services shall not, in the regular course of business, monitor content of Information Resources on the network. However, suspicious aggregate behavior or requests from authorities can cause activities on the network to be reviewed. It is the right of U.T. System Administration to monitor and review any activities on their resources. It is best, therefore, to assume all actions taken are the not private.

29. Disciplinary Actions

Misuse or destruction of Information Resources can vary in severity and appropriate disciplinary actions should be taken in proportion to the incident. It is not the role of Information Technology professionals to impose discipline, but it is their role to monitor resources, to identify potential incidents and to bring such incidents to the attention of executive management. The following guidelines apply:

- Suspected incidents involving employee misuse should be brought to the attention of the appropriate departmental management.
- If an investigation involving review of the content of an employee's files is required, written permission will be obtained from an executive officer.
- If it is determined that a misuse violation has occurred by an employee, this should be brought to the attention of the employee's departmental management, the Office of Human Resources and, in the case of criminal violation, the Office of Director of Police.
- Violations by non-employees will be referred to the appropriate authorities. The Office of General Counsel will be contacted to provide direction in terms of identifying the appropriate authority.

30. Removal, Re-Deployment, and Disposal of Equipment and Media

- **Removal of Equipment and Portable Electronic Media**
 - System Administration staff shall not remove from System Administration's facilities equipment or portable electronic media containing sensitive information (e.g., protected health information (PHI), social security numbers (SSN), credit card numbers) without the approval of the Information Security Officer, his/her designee, or departmental manager. Approval shall only be granted if the equipment or portable electronic media containing sensitive information is necessary for the performance of business related functions and the data is protected from unauthorized disclosure (e.g., encrypted, etc.).
 - System Administration staff shall complete an Equipment Removal Request form annually to remove equipment and/or portable electronic media from System Administration facilities.
 - System Administration Departments with equipment and portable electronic media containing sensitive information under their care shall maintain a log of all approved removal of equipment and portable electronic media containing sensitive information. The log should include:
 - Name of staff removing the equipment and/or media
 - Item being removed
 - Justification for the request

- Person approving the request
- Signature and date of request.
- Date equipment and/or media returned
- The staff member shall:
 - Return the equipment or electronic media when functions are completed
 - Report immediately to departmental manager the loss of any equipment, portable electronic media, or any sensitive data stored in them.
- System Administration staff shall not download or make convenience copies of sensitive information from UT System mainframes or System Administration network servers into local desktop hard drives or portable electronic media (e.g., PDAs, thumb drives, floppy drives, CDs) unless the portable electronic media is used as part of System Administration's data back-up procedures or disaster recovery and the data is protected from unauthorized disclosure (e.g., encrypted, etc.).
- **Re-Deployment and Disposal of Equipment and Portable Electronic Media**

All sensitive information shall be removed from equipment or re-writable portable electronic media by using a method that ensures that it cannot be recovered or reconstructed before re-deployment, disposal and/or surplus of equipment. However, if the media is re-used as part of System Administration's data back-up procedures or disaster recovery, such media shall not be subjected to these procedures before re-use.

 - **Equipment:** System Administration Departments shall be responsible for the re-deployment, disposal, and/or surplus of equipment under their care that contains sensitive information. OTIS shall be responsible for the re-deployment, disposal, and/or surplus of servers and server-attached storage devices.
 - Departments shall contact the OTIS Helpdesk to re-deploy, dispose and/or surplus of equipment containing sensitive information. Equipment should stay in the department.
 - Departments shall identify applications and/or files containing sensitive information stored in equipment being re-deployed, disposed of, and/or surplus.
 - Helpdesk technical staff shall back up all previously identified applications and/or files containing sensitive information to a computer, tape, CD, or other storage media before equipment is re-used or relocated, disposed and/or surplus and validate the accuracy, completeness, and integrity of the back-up.
 - Helpdesk technical staff reformats and overwrites the hard drive using a hard disk formatting utility designed to prevent the recovery and reconstruction of deleted data.
 - If equipment is being re-deployed, the department is responsible for completing and signing the Report of Transfer of Equipment form.
 - If equipment is being disposed and/or surplus, the helpdesk technical staff is responsible for signing-off on the Inventory Form and departments are responsible for making arrangements for Facilities Services to pick up the equipment.
 - **Portable Electronic Media:**
 - System Administration Departments are responsible for removing all sensitive information from re-writable portable electronic media before the media is re-used.
 - Department staff shall reformat and overwrite the media containing sensitive information to the level that the sensitive information cannot be recovered or reconstructed before the media is re-used.
 - If the media cannot be reformatted to the level that the sensitive information cannot be recovered or reconstructed, department staff shall dispose of the media according to the procedures established below.
 - Departments are responsible for the disposal of portable electronic media that contains sensitive information.
 - Departments shall physically destroy or damage the media containing sensitive information to the level that the media is no longer usable and the sensitive information cannot be recovered or reconstructed

31. *Incidental Use*

Incidental use of Information Resources is authorized per the Information Security Policy. The Office of Technology and Information Services is permitted to monitor the incidental personal use of Information Resources to ensure that:

- Use is restricted to U.T. System Administration employees only.
- Use does not result in a direct cost to U.T. System Administration.
- Storage of any non-work related email messages, voice messages, files and documents within the email system is less than 5% of a User's mailbox space.
- Non-work related files are not stored on network file servers.

32. *Sharing Documents with External Entities*

When providing documents to third-parties it is critical to remove all hidden metadata (comments, tracking, prior saved information, identities, etc) before transmission. This can be done by using add-on tools to Office products or by using Office 2007 and invoking Document Inspector before sharing. This must also be done prior to the conversion of a document to .pdf form as no mechanism for removing data from this format exists.

APPENDIX 1 - Definitions

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

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 Office of Technology and Information Services (OTIS) acts as custodian of network resources at U.T. System Administration.

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.

Change:

- any implementation of new functionality.
- any interruption of service.
- any repair of existing functionality.
- any removal of existing functionality.

Computer Incident Response Team (CIRT): Personnel responsible for coordinating the response to computer security incidents in an organization.

Confidential: The Classification of data of which unauthorized disclosure/use could cause serious damage to an organization or individual.

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

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

Electronic mail (email): Any message, image, form, attachment, data, or other communication sent, received, or stored within an electronic mail system

Email: Abbreviation for electronic mail.

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

Encryption: The application of a specific algorithm to data so as to alter the appearance of the data to make it incomprehensible to those who might attempt to "steal" the information.

Decryption: The process of decryption applies the encryption algorithm in reverse to restore the data to its original appearance.

FTP (File Transfer Protocol): An IP application protocol for transferring files between network nodes or computers.

Information Resources (IR): any and all computer printouts, online display devices, mass 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 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 facilities: Any location that houses Information Resource equipment (includes servers, hubs, switches, and routers). Facilities are usually dedicated rooms or mechanical/wiring closets in the buildings.

Information Resources Manager (IRM): 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 Information Resource Manager 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 Information Resource Manager, the title defaults to the agency's Executive Director, and the Executive Director is responsible for adhering to the duties and requirements of an Information Resource Manager.

Information Security Officer (ISO): Responsible to the Information Resource Manager 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. If an Information Security Officer is not designated, the Information Resource Manager serves in this capacity.

Integrity: The accuracy and completeness of information and assets and the authenticity of transactions.

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.

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.

Office of Technology and Information Services (OTIS): The name of the U.T. System Administration department responsible for computers, networking, data management and other Information Resources.

Offsite Storage: Based on data criticality, offsite storage should be in a geographically different location from the U.T. System Administration campus that does not share the same disaster threat event. Based on an assessment of the data backed up, removing the backup media from the building and storing it in another secured location on the U.T. System Administration Campus may be required.

Owner: The manager or agent responsible for the function that is supported by the resource or the individual upon whom responsibility rests for carrying out the program that uses the resources. The owner is responsible for establishing the controls that provide the security. 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.

Password: A string of characters used to verify or "authenticate" a person's identity.

Portable Computing Devices: Any easily portable device that is capable of receiving and/or transmitting data. These include, but are not limited to, notebook computers, handheld computers, PDAs (personal digital assistants), pagers, and cell phones.

Production System: The system environment comprised of hardware, software and data in which an organization's data processing is accomplished.

Scheduled Change: Formal notification received, reviewed, and approved by the review process in advance of the change being made.

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 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.

Sensitive Information: Information maintained by state agencies that requires special precautions to protect it from unauthorized modification or deletion. Sensitive information may be either public or confidential. It is information that requires a higher than normal assurance of accuracy and completeness. The controlling factor for sensitive information is that of integrity.

Server: A computer program that provides services to other computer programs in the same, or another, computer. A computer running a server program is frequently referred to as a server, though it may also be running other client (and server) programs.

S-HTTP (Secure HTTP): An extension to the HTTP protocol to support sending data securely over the World Wide Web. S-HTTP is designed to send individual messages securely.

SSL (Secure Sockets Layer): A protocol for transmitting private documents via the Internet. SSL works by using a private key to encrypt data that's transferred over the SSL connection. Many Web sites use the protocol to obtain confidential user information, such as credit card numbers. By convention, URLs that require an SSL connection start with https: instead of http:.

Strong Passwords: A strong password is constructed so that it cannot be easily guessed by another User or a "hacker" program. It is typically a minimum number of positions in length and contains a combination of alphabetic, numeric, or special characters.

System Administrator: Person responsible for the effective operation and maintenance of Information Resources, including implementation of standard procedures and controls, to enforce an organization's security policy.

Terminal Services: A Terminal Services server can host multiple secure simultaneous client sessions. Applications run on the server, client has remote desktop capability and is sent secure screen updates.

Trojan Horse: 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 email or on a diskette or CD, often from another unknowing victim, or may be urged to download a file from a Web site or bulletin board.

Unscheduled Change: Failure to present notification through the review 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.

User: An individual, automated application or process that is authorized by the owner to access the resource, in accordance with the owner's procedures and rules. Has the responsibility to (1) use the resource only for the purpose specified by the owner, (2) comply with controls established by the owner, and (3) prevent disclosure of confidential or sensitive information. The user is any person who has been authorized by the owner of the information to read, enter, or update that information. The user is the single most effective control for providing adequate security.

Vendor: someone outside U.T. System Administration who exchanges goods or services for money.

Virus: A program that attaches itself to an executable file or vulnerable application and delivers a payload that ranges from annoying to extremely destructive. A file virus executes when an infected file is accessed. A macro virus infects the executable code embedded in Microsoft Office programs that allows users to generate macros.

VPN (Virtual Private Network): A network that is constructed by using a public network (the Internet) to connect computers. VPN systems use encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted.

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.

Website: 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

World Wide Web: Also referred to as the Web is a system of Internet hosts that supports documents formatted in HTML (Hypertext Markup Language), which contains 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. A worm is 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.

APPENDIX 2 – Strong Password Guidelines

Introduction

Passwords are a means of controlling access to Information Resources. Unauthorized access can compromise information confidentiality, integrity and availability resulting in loss of revenue, liability, loss of trust or embarrassment to U. T. System Administration. U. T. system Administration's security policy calls for the use of strong passwords to ensure password confidentiality and protect the data at System Administration. Password requirements:

All passwords, including initial passwords, must be constructed, implemented, and maintained according to the System Administration password policy. Passwords must:

- Be changed at least annually
- Be changed immediately if the security of the password is in doubt
- Be treated as confidential information
- Have a minimum length of 8 characters
- Be comprised of a combination of alpha, numeric or special characters
- Not contain a word of 4 letters or more which is found in the UT System dictionary
- Be encrypted when stored or transmitted

Definitions

Strong Password: A strong password is constructed so that another user or a "hacker" program cannot easily guess it. It is typically a minimum number of positions in length and contains a combination of alphabetic, numeric, or special characters. Combine short, unrelated words with numbers, special characters, or mixed case. For example: eAt42peN

Constructing a Strong Password

System Administration has adopted Microsoft's strong password implementation and added to it a commonly used Higher Education Dictionary Check. A dictionary check compares the password or any string of letters in the password to see if it contains a word found in the dictionary. For example, the password 1loveJohn! would be blocked because the word "love" and the name "John" are in the dictionary. The dictionary check is for any word of 4 characters or more. It also blocks passwords that substitute numbers for letters in words found in a dictionary, such as 1 for l and 0 for O (e.g. l0ve). Several other checks are made such as words spelled backwards and two words repeated in succession.

To construct a strong password you must use 3 of the following character sets and have a minimum of 8 characters:

- Upper case letters (A – Z)
- Lower case letters (a – z)
- Numbers (0-9)
- Special Characters (#\$%&* etc)

Examples:

2BorNot2B
*TT4now!
Gre@td@y

Common way to pick complex passwords

The most successful method for picking a password that is robust but easy to remember is to select a phrase and let it inspire the password. It can be the cute phrase your child just said, a line from a song or poem you love or a quote from the boss. For example:

"To be or not to be. That is the question." = 2bon2bTil?
"We don't need no education. We don't need no thought control" = Wdn0eWdn0tc"
"Rudolf the red-nosed reindeer had a very shiny nose" = Rtrrhavsn!

Details about the Dictionary Check

Many people attempt to disguise a dictionary word by adding random characters at the beginning or end of the word. The system automatically screens for this technique. For example, the passwords below would not be allowed no matter what X or XX is:

TexasXX
TexasX
XTexas
XXTexas
XXTexasXX

Non-Letters As Letters

Many people try to use certain non-letters as letters within their passwords. The system automatically translates all of the following non-letters into letters before looking up words in its dictionary:

\$ = s 4 = h 2 = a 3 = e 0 = o 1 = l 1 = i

Passwords like Texa\$ would therefore be rejected.

Capitalization

Passwords are case-sensitive: uppercase and lowercase letters are considered to be separate letters (except at the beginning of a word). Capitalizing random letters in a dictionary word (caRpoRTS) will not, however, fool the screening program. The point is to capitalize letters in a non-word password, in order to provide another layer of complexity against other password-cracking programs.

Obvious Tricks

The system automatically screens out passwords set in the following manner:

- Passwords based on a dictionary word spelled backward (drofnats).
- Passwords based on two dictionary words in a row (dogdog).
- Passwords based on the person's login name.
- Passwords that are all white space.
- Passwords that contain control characters.
- Passwords that are all numbers.
- Passwords followed and/or preceded by 1 or 2 characters (9cheval, cheval9, 99cheval, cheval99, 99cheval99 etc.)
- Passwords with several repeating characters (aaaaaaa or aaaabbbb or abababab).
- Passwords that do not have more than four characters that differ from the previous character by one (1234abcd).
- Passwords with license plate patterns (daaadd).
- Passwords with social security patterns (dddssddd).
- Passwords with phone number patterns (dddssddd or ddddssddd).

Strong Password Guidelines

Passwords should **not** be easily related to such personal information as:

- your username or logon ID your employee number
- your given name
- names of family, friends, pets, co-workers, fantasy characters, etc.
- your nickname
- your social security or driver's license number
- your birthday
- your license plate number
- your address or street name
- your phone number
- the name of your town or city
- the name or abbreviation of your company or department

- computer terms and names, commands, sites, companies hardware, software, etc.
- common industry terms or acronyms
- word or number patterns such as aaabbb, zyxwvut, 123321, etc.
- makes or models of vehicles
- slang words
- obscenities
- technical terms
- school names, school mascot, or school slogans
- any information about you that is know or is easy to learn (favorite - food, color, sport, etc.)
- any popular phrases, acronyms, jargon, etc.
- words that appear in a dictionary (English or foreign)
- the reverse of any of the above
- the same as other passwords selected for personal use outside of the office, or passwords commonly used on public web sites

Application Passwords:

The application environment at System Administration consists of web applications hosted on the mainframe at Austin, terminal emulation applications hosted on the mainframe, Access database applications hosted on the local area network, applications that are hosted by outside providers, and web applications hosted locally. Some of the latter use Access databases for data storage and some use SQL Server for data storage. Authentication methods for each of these application types occurs in a slightly different way, with some variation depending on what the particular technology allows.

In all cases, the password does not display while it is being entered, and web-based login occurs over an SSL connection. Overall, however, applications hosted at System Administration have not been written to enforce a strong password.

Now that password standards have been defined, the long term plan is to rewrite the logins for existing applications to authenticate against LDAP or Active Directory, and to develop new applications to use this once those technologies are in place. Password standards could then be enforced through those services. We regard this as a more efficient and reliable means of ensuring consistency in standards than having each application enforce standards independently.

APPENDIX 3 - Encryption Guidelines

Introduction

Encryption refers to the transformation of plain text into cipher-text to protect it. Encryption guards against theft or accidental disclosure of confidential or sensitive information. Encryption is used to protect against eaves-dropping, it renders information private by making it unreadable to all except those who have the key needed to decrypt the data. These encryption guidelines are to be used by System Administration employees or individuals who transmit System Administration confidential or personally identifiable information (data that is required to be protected by HIPAA, FERPA, Gramm-Leach-Bliley, or other law) across unsecured networks (like the Internet) or for storage on unsecured workstations or portable devices.

There are risks associated with the encryption of data. There is the possibility that a key to decrypt the data may be lost rendering information or university records “unreadable” and “unrecoverable.” Proper procedures should be in place to protect encryption keys from exposure and/or loss. Encryption should only be used in certain circumstances.

U. T. System Administration servers are protected by multiple layers of security; therefore, data stored on System Administration servers should not be encrypted unless determined necessary through risk assessment. When at all possible, all System Administration data (files) should be stored on System servers (these files can be accessed remotely via secure VPN or Terminal Services). Encrypted files should **not** be stored in System Administration’s document management system (FileNet).

When to Use Encryption

Transfer of Confidential or Sensitive Information to or from a Person or Entity Outside of System Administration -

Encrypted email or secure FTP must be used for official University business when transmitting information of a sensitive, private or confidential nature (including information protected by HIPAA or FERPA) across a public network.

All System employees should use a University of Texas System assigned Verisign certificate to encrypt email containing sensitive or confidential information transmitted across unsecured networks. Email encryption requires that you have the public key of the individual to whom you are sending an encrypted message. All System component institutions have access to Verisign certificates. One may obtain a public key in a number of ways. When you receive a digitally signed message, you receive the sender's public key. Mail clients may automatically store the public keys of all senders in Outlook Contacts. You may have to selectively choose to save an individual's public key. An individual's public key may also be obtained from a directory service (VeriSign's Directory Service). Detailed instructions on encrypting mail with this method can be found on the Helpdesk information web page.

Another method of transferring confidential or sensitive information to an outside entity or person is by the use of secure FTP (SFTP). OTIS is currently running a SFTP server which works with most free SFTP clients. Before using any secure FTP client, please read license agreement before downloading software. Contact OTIS for additional information regarding SFTP.

Confidential or sensitive information residing on web servers or collected via web applications should be protected. Protection of data or information residing on a web server should be in accordance with risk assessment and, at a minimum, SSL or Secure HTTP (S-HTTP) should be deployed. If there is a need to

communicate sensitive data to a party that is unable to accept encrypted files for technical reasons, the information should be communicated using alternative means such as US mail or telephone.

Storage of Confidential or Sensitive Information on User Computers and Devices:

Desktop Computer Storage:

All desktops (including portable computers used as desktops) connected to the U. T. System Administration network have access to centrally controlled servers. All University business related data files created or modified by these computers must be stored only on the centrally managed servers and not on a local hard drive. In certain cases where personally identifiable information or sensitive information may be temporarily be cached or saved on a local drive, SafeBoot software may be installed to encrypt the local drive (OTIS maintains and supports the use of this encryption software) on “high risk” computers.

Portable Devices or Removable Media:

All sensitive or confidential data or files stored on a portable device (such as a laptop or PDA) or removable media (CD's, thumb drives, etc) must be encrypted using SafeBoot software. Examples of information that should always be encrypted includes but is not limited to:

- personally identifiable information (SSN, Drivers License, date of birth, credit card information)
- data which pertains to an individual's race, religion, or national origin
- data that describes the state of an individual physical or emotional well-being
- data that describes the methods or procedures used to safeguard assets or maintain the integrity of a system, application or network
- information protected by the Federal Educational Rights and Privacy Act (FERPA)
- information protected by Health Insurance Portability and Accountability Act (HIPAA)
- information relating to sensitive negotiations and research or other University business

As a precaution against accidental exposure of university data; all portable computing devices (laptops, tablet computers etc.) will be encrypted using SafeBoot software. Any university records on portable devices or saved on removable media is required to be backed up in an unencrypted form (unless encryption is warranted based on risk assessment) in a secure location on a network server.

Before international travel; you may need to check the laws pertaining to countries with encryption restrictions (e.g., some countries may inspect computer software upon departure; and some equipment and software have been confiscated because of the data contained or due to software encryption, which is standard in many programs.).

If you are uncertain about whether data on your local drive should be encrypted or if data on your portable device is encrypted please contact the OTIS helpdesk or the Network Security Officer or OTIS management.

APPENDIX 4 – Minimum Standards for Portable Computing

The following minimum standards for portable computing at System Administration apply:
Computer capable of running Windows XP

<i>Minimum</i> Requirements for Windows XP (Performance enhanced by more memory and larger hard disk)	
Computer/Processor	500 MHz or higher Pentium-compatible CPU.
Memory	At least 256 megabytes (MB) of RAM; more memory generally improves responsiveness.
Hard Disk	10 GB with 650 MB free space.
CPU Support	Windows XP Professional supports single and dual CPU systems.
Drive	CD-ROM or DVD drive.
Display	VGA or higher resolution monitor.
Keyboard	Required.

- For Dialup purposes - external or internal modem capable of 56k V.92.
- Current Virus Protection software (available from the Office of Technology and Information Services)
- Password Protected screen saver (activation set at 10 minutes or less)
- For DSL or Cable modem subscribers the following standards apply:
 - Personally owned computers must connect via Terminal Services
 - Cisco VPN client (provided by OTIS) available for University owned equipment
 - Must use software firewall (provided by OTIS)

APPENDIX 5 –Project Management Guidelines

Purpose:

This procedure establishes guidelines for conducting outlining the appropriate amount of structure to manage the risks in cost, time and quality for each Information Resource projects.

Scope:

These guidelines apply to all Information Resource Projects initiated at U.T. System Administration.

Project Definitions:

U.T. System Administration works to ensure that all Information Resource projects within System Administration meet quality assurance standards and that projects are delivered on time, within budget, and meet user needs. However, since projects vary widely in their scope and impact, System Administration does not believe it is appropriate to apply the same level of assessment and monitoring to all projects: in some cases, the effort required for quality assessment and project planning could easily exceed the development effort.

System Administration therefore adheres to what it considers to be project management guidelines that are efficient, manageable, and meaningful to the State, the University, and its constituents. Each project that requires involvement of Information Resource staff is evaluated in terms of its cost, scope, and risk level. Different levels of project management guidelines are applied based upon the project classification.

Projects are evaluated in terms of the following:

Low Risk Projects:

Budget/Effort: < \$200,000 and **Timeline:** < 6 months and **Staff:** < 2 staff

Impact: Involves only U.T. System and Components

The vast majority of projects within System Administration are of limited scope and involve a minimal expenditure of resources and effort. Most projects requested are intended to automate departmental business processes and do not involve a project team or an extended timeline.

While these applications are critical to the requestors and to the efficiency of System Administration, they have extremely limited scope, development time, and impact outside of U.T. System.

High Risk Projects:

Budget/Effort: > \$200,000 or **Timeline:** > 6 months or **Staff:** 2 or more staff, or vendor

Impact: Significant impact outside of agency

Although such projects are quite rare within System Administration, a project determined to be of high risk is subject to a higher level of scrutiny and monitoring. When they do arise, a special oversight committee is appointed to guide the project development, status reports, and to keep management fully apprised

In addition, Projects should be reviewed using the Project Sizing Tool identified by UTS140. Any project which is identified as Large must adhere to the requirements laid out in that Policy and adhere to the Project Management Process for High Risk Projects

Project Management Process:

Evaluate Risk:

1. Business unit contacts the manager in charge of analysts and programmers to make the initial request for assistance and resources.

2. A preliminary review of risk is done based on size, cost and complexity of initiative. When appropriate, in compliance with UTS140, OTIS completes the Project Sizing Tool to determine project management requirements.
3. Director of OTIS makes final evaluation of the risk of the initiative.

Low Risk Project:

1. Manager of Information Services makes initial determination of the project requirements and assigns to a programmer. These requirements are documented as part of the Project List system.
2. Programmer meets with requestor to complete functional specifications and updates entry in the Project List for the work group. The Programmer is responsible for maintaining this project entry up to date, attaching any relevant information on scope, requirements, etc. which will inform the work group.
3. Manager of Information Services monitors development progress to ensure on-time delivery and becomes involved with defining functional requirements or adjusting scope as needed. Programmer alerts manager to any potential problems.

High Risk Projects:

1. System advocate prepares a Project Charter for consideration by review and approval groups.
2. Director of OTIS meets with System Advocate to discuss goals, objectives, and budget.
3. IT Governance Board appoints Advisory Committee for the project, comprised of representatives from across System Administration and possibly from components, depending upon the project.
4. Advisory committee evaluates alternative approaches and solutions, including consideration of vendors, outsourcing, etc.
5. If relevant, vendor presentations are scheduled and evaluated by the advisory committee.
6. Advisory committee develops a formal recommendation to submit to executive management.
7. During the project lifecycle formal documentation of the following topics must be created and standards laid out in the following knowledge areas:
 - integration management;
 - scope management;
 - schedule management;
 - cost management;
 - quality management;
 - resources management;
 - communications management;
 - risk management; and
 - procurement (acquisition) management.

NOTE: Model documents posted at <http://www.dir.state.tx.us/pubs/framework/index.htm> should be used

APPENDIX 6 – Sample Memorandum of Understanding

Information Technology Employee Memorandum of Understanding

Print Employee Name

Employee EID

Business Procedure 53-02-96 defines a position of special trust as 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. U. T. System Administration employees who support information technology hold such positions in that their responsibilities may bring them into contact with sensitive information and they are charged with protecting University of Texas Information Resources. It is imperative that these employees perform their duties in a most professional and ethical manner.

The University of Texas System Administration *Information Resources Security Operations Manual* requires that Information Technology employees sign a memorandum of understanding relating to their custodial role and responsibilities.

Note the following principles of conduct:

- Information Technology employees are bound by the provisions of *BPM 53-06-05 – Policy for the Use and Protection of Information Resources*, the System Administration *Information Resources Use and Security Policy*, *Information Resources Security Operations Manual*, and *Information Resources Acceptable Use Policy*. Holding positions of special trust, these employees are expected to set an example for others in terms of proper handling of information resources.
- Except as required by law or University policy, technical employees should not disclose information regarding University owned systems or other information that can prove detrimental to operations or compromise system security. Additionally, except as necessary to execute work responsibilities and enforce policy or law, technical staff should not disclose information about University operations learned through the performance of support duties.
- If during performance of duties an employee observes violations of laws relating to use of information resources, the employee is to report such incidents to management. Further actions will be taken as appropriate in accordance with provisions outlined in *BPM 53-02-96 – Policy for the Use and Protection of Information Resources*.
- It is imperative that technical employees retain the trust of those served. Respect for confidentiality is the foundation for such trust. Therefore, to the extent possible, the monitoring of network and system logs and directories is to be done in the least intrusive manner possible. Employees are not allowed to read the contents of user files or electronic mail messages without user permission. Exceptions are governed by *BPM 53-02-96 – Policy for the Use and Protection of Information Resources* and must be made in compliance with that policy.
- To protect University Information Resources, technology support employees are authorized to temporarily remove from service any hardware or software system that is in jeopardy or poses a threat to other systems.

I acknowledge that I have read and understand that I must comply with the principles of conduct and policies above.

Employee Signature

Date