## Contents

- Introduction ................................................................. 1
- General Policy Statement ........................................... 2
- Scope ............................................................................... 2
- Definitions ....................................................................... 2
- Data Classifications .................................................... 3
- Privacy Statement ......................................................... 4
- Specific Policy Statements ........................................... 4
- Key Roles and Responsibilities ................................... 7
- Statutory Authority ....................................................... 8
- How You Can Help ....................................................... 9
- Failure to Comply (Individually) ............................... 11
- Failure to Comply (Institutionally) ......................... 12
- Conclusion .................................................................... 13
- Further References .................................................... 13
- Information Resources Security Acknowledgment and Nondisclosure Agreement .............................. 15
Introduction

All information and information resources (IR) managed by UTMB are strategic and vital assets belonging to the people of Texas, and we will not betray the trust that they have given to us. To ensure this, UTMB has established a comprehensive IR Security Program that responds to requirements of the Texas Administrative Code 1 TAC §202 (Information Security Standards) and the State of Texas Department of Information Resources’ Practices for Protecting Information Resources Assets. The Information Security Officer (ISO) is responsible for coordinating the IR Security Program.

The strategies outlined within this manual provide a reasonable approach for reducing information security risks. Included is an overview of the policies and major laws, role and responsibility descriptions to provide a perspective of the functional involvement of all personnel within the UTMB IR security program, data classification descriptions to identify UTMB’s approach to confidential and sensitive information protection efforts, and suggested security practices and repercussions related to failure of compliance.

Our intent is not to simply inform personnel of present computer crime laws and associated consequences, but to create an organizational culture that is conducive to information security. Since employees are potentially the most effective line of defense in ensuring the security of IR, we would rather use this initiative to cultivate a staff with an intense, sincere attitude toward the importance of IR and the need to protect its security and quality.

Regardless of the size or nature of any of UTMB’s IR, the following major security objectives must be met.

- **Confidentiality** of personal, proprietary, or otherwise sensitive data entered into, or processed by, the system;

- **Integrity** and accuracy of data, its source, its destination, and the processes applied to it; and

- **Availability** of reliable systems and the data or services they support.

If these objectives are met, then other assets that are involved with or dependent upon the information being protected will also be protected.

For example, meeting these goals will, in general, ensure that the physical equipment itself is protected from unauthorized access or damage.
It is further incumbent that:

- IR security is everyone’s personal responsibility;
- Compromising IR security, whether accidental or intentional, will result in disciplinary action;
- Access to information assets will be limited to the minimum necessary to accomplish the intended purpose of use; only a small portion is truly “public”; and
- Unlawful breach of IR security may result in state and/or federal prosecution.

The program is designed to benefit all UTMB faculty, students, staff, and supporting contractor personnel, and can succeed only through joint effort. Although the program itself will continue to mature, our best defense is always a well informed user; therefore, your cooperation is absolutely essential.

**General Policy Statement**

It is the policy of UTMB to protect the information resources assets of the state of Texas in accordance with the State of Texas Department of Information Resources' (DIR) *Practices for Protecting Information Resources Assets* as published in the Texas Administrative Code 1 TAC §§202 (Information Security Standards), and as authorized by the Information Resources Management Act (Chapter 2054, Texas Government Code Annotated).

**Scope**

The IR Security Policy applies to all information obtained, created, or maintained by UTMB’s automated IR. This policy applies equally to all levels of management and to the personnel they supervise. Further, this policy applies to all information generated by the UTMB IR functions through the time of its transfer to ownership external to UTMB or its proper disposal/destruction. This policy applies to all personnel including UTMB employees, students, agents, consultants, or any other individuals whose services are procured by a contract or through a temporary personnel agency.

**Definitions**

The term *information* is defined as any and all data, regardless of form, that is created, contained in, or processed by, UTMB IR facilities, communications networks, or storage media.
**Information Resources** is defined as 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, handheld computers, personal digital assistants (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.

**Data Classifications**

*Confidential* information is the classification of data that is exempt from disclosure under provisions of the Texas Public Information Act or other applicable state or federal law, regulation, or court order. The controlling factor for confidential information is prevention of dissemination.

One way to determine the confidentiality of data is to ask the questions “Is it personal or proprietary in nature? If disclosure should be based upon a business need to know, then the data is confidential and should have adequate security controls to restrict disclosure.

*Sensitive* information is the classification of data requiring special precautions to protect it from unauthorized modification or deletion. It may be either public or confidential but requires a higher than normal assurance of accuracy and completeness. The controlling factor for sensitive data is assuring and maintaining integrity.

One way to determine the sensitivity of data is to ask the questions “What will it cost if the data is wrong?, manipulated for fraudulent purposes?, not available?, given to the wrong person?"

University of Texas System, UTS 165 – Information Resource Use and Security Policy requires protecting “Sensitive Digital Data” which includes social security numbers, Protected Health Information (PHI), sensitive research data, digital data associated with an individual and/or digital data protected by law.

Under UTS 165, data elements (names, SSNs, etc.) used, stored or displayed collectively which can uniquely identify an individual are classified and must be protected as Sensitive Digital Data.
Privacy Statement

Electronic files created, sent, received, or stored on IR owned, leased, administered, or otherwise under the custody and control of UTMB are not private and may be accessed by appropriate personnel in accordance with the provisions and safeguards provided in the Texas Administrative Code 1 TAC §§202 (Information Security Standards), Information Resource Standards and in the University of Texas System Policy 165 - Information Resource Use and Security Policy (UTS 165).

Specific Policy Statements

Specifically, UTMB will apply policies, practice standards, and procedures to protect its IR functions from internal data or programming errors and from misuse by individuals within or outside the university. This is to protect UTMB from the risk of compromising the integrity of state programs, violating individual rights to privacy and confidentiality, violating criminal law, or potentially endangering the public’s safety.

1. All UTMB IR security programs will be responsive and adaptable to changing technologies affecting UTMB IR hence IR security controls must not be bypassed or disabled.

2. Security awareness of personnel must be continually emphasized, reinforced, updated, and validated.

3. All users of IR are responsible for managing their use of IR and are accountable for their actions relating to IR security. Personnel are also equally responsible for reporting any suspected or confirmed violations of this policy to the appropriate management or to the UTMB Compliance Hotline at (800) 898-7679.

4. Passwords, Personal Identification Numbers (PIN), security tokens (e.g., Smartcard), and other computer systems security procedures and devices shall be protected by the individual user from use by, or disclosure to, any other individual or organization.

5. Access to, change to, and use of UTMB IR must be strictly secured. Information access authority for each user must be reviewed on a regular basis, as well as each job status change such as: a transfer, promotion, demotion, or termination of service.

6. The use of UTMB IR must be for officially authorized UTMB business purposes only. Departments responsible for the custody and operation of computers (custodian departments) shall be responsible for proper authorization of UTMB IR utilization, the establishment of effective use, and reporting of performance to management.
7. Some information is confidential and must be guarded against unauthorized disclosure; other information is sensitive and must be protected from unauthorized modification. Some information is both confidential and sensitive.

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

9. On termination of the relationship with UTMB, users must surrender all property and IR managed by UTMB. All security policies for UTMB IR apply to and remain in force in the event of a terminated relationship until such surrender is made.

10. The owner must engage the Information Resources Manager (IRM) or designee, at the onset of any project to acquire computer hardware or to purchase or develop computer software. The costs of acquisitions, development and operation of computer hardware and applications must be authorized by appropriate management. Management and the requesting department must act within their delegated approval limits in accordance with the UTMB authorization policy. A list of standard software and hardware that may be obtained without specific, individual approval will be published.

11. The department which requests and authorizes a computer application (the owner) must take the appropriate steps to ensure the integrity and security of all programs and data files created by, or acquired for, computer applications. To ensure a proper segregation of duties, owner responsibilities cannot be delegated to the custodian (e.g., Accounting, Invision, ClinWeb, Pathology, Research Administrative Services, as owners, cannot delegate ownership responsibilities to Information Services, a custodian.)

12. The UTMB IR network is owned and controlled by UTMB IS. Approval must be obtained from IS before connecting a device that does not comply with published guidelines to the network. IS reserves the right to remove any network device that does not comply with UTMB practice standards or is not considered to be adequately secure.

13. The sale or release of computer programs or data, including email lists and departmental telephone directories, to other persons or organizations must comply with all UTMB legal and fiscal policies and procedures.

14. The integrity of general use software, utilities, operating systems, networks, and respective data files are the responsibility of the custodian department. Data for test and research purposes must be de-personalized prior to release to testers unless each individual involved in the testing has authorized access to the data.

15. All changes or modifications to UTMB IR systems, networks, programs or data must be approved by the owner department that is responsible for their integrity.

16. Custodian departments must provide adequate access controls and system monitoring to protect data and programs from misuse in accordance with the needs defined by owner departments. Access must be properly documented, authorized and controlled.

17. Sensitive data will not be removed from the premises of UTMB
without appropriate authorization from the data owner. If approved, the data must be protected from loss and unauthorized disclosure through the use of strong passwords and encryption.

18. All departments must carefully assess the risk of unauthorized alteration, unauthorized disclosure, or loss of the data for which they are responsible and ensure, through the use of monitoring systems, that UTMB is protected from damage, monetary or otherwise. Owner and custodian departments shall have appropriate backup and contingency plans for disaster recovery based on risk assessment and business requirements.

19. All computer systems contracts, leases, licenses, consulting arrangements or other agreements must be authorized and signed by an authorized UTMB officer and must be approved as to form by the Legal Department.

20. UTMB IR computer systems and/or associated equipment used for UTMB business that is conducted and managed outside of UTMB control must meet contractual requirements and be subject to monitoring.

21. External access to and from UTMB's IR must meet appropriate published UTMB security guidelines.

22. All commercial software used on computer systems must be supported by a software license agreement that specifically describes the usage rights and restrictions of the product. Personnel must abide by all license agreements and must not illegally copy licensed software. The IRM through IS reserves the right to remove any unlicensed software from any computer system.

23. The IRM through IS reserves the right to remove any non-business related software or files from any system.

24. Adherence to all other policies, practice standards, and procedures issued in support of these policy statements is mandatory.
Key Roles & Responsibilities

**Chief Administrative Officer (CAO):** Responsible for establishing and maintaining an information security and risk management program for all information resources within the university. (President)

**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. For mainframe applications, Information Services is the custodian; for micro and mini applications, the owner or user may retain custodial responsibilities. The custodian is normally a provider of services.

**Information Resources Manager (IRM):** Responsible to the CAO and the State of Texas for management of UTMB’s information resources. UTMB’s IRM is the Chief Information Officer. The designation of an agency information resources manager is intended to establish clear accountability for setting policy for information resource 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 UTMB President, the President’s Council, and the State of Texas to implement Security Policies, Procedures, Practice Standards and Guidelines to protect the Information Resources of UTMB.

**Information Security Officer (ISO):** Responsible to the IRM for administering the information security function within UTMB. The ISO is UTMB’s internal and external point of contact for all information security matters. (Information Services)

**Information Security Administrator (ISA):** Responsible to the ISO for administering the information security function within a specific department.

**Information Services (IS):** The name of the UTMB department responsible for computers, networking and data management.

**Internal Auditor:** Ensures that UTMB information resources are being adequately secured, based on risk management, as directed by the CAO or the IRM acting on delegated authority for risk management decisions.

**Owner:** The manager or agent responsible for the function which is supported by the resource, 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.
**Program Manager:** Assigned IR ownership, responsible for the information used in carrying out program(s) under their direction and provides appropriate direction to implement defined security controls and procedures. (Materials Management, Human Resources, Research Administrative Services, Correctional Managed Healthcare, Library, etc)

**Technical Manager:** Assigned custodians of IR, provide technical facilities and support services to owners and users of information. Assists Program Management in the selection of cost effective controls to be used to protect information resources. Are charged with executing the monitoring techniques and procedures for detecting, reporting, and investigating breaches in information asset security.

**User:** 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 to read, enter, or update information by the owner of the information. The user is the single most cost effective control for providing adequate security.

**Statutory Authority**

**Family Educational Rights and Privacy Act of 1974 (FERPA):** Protects the privacy of student education records.

**Copyright Act of 1976, as amended:** Provides for copyright ownership and protection against infringement.


**Sarbanes-Oxley Act of 2002 (SOX):** Requires effective internal control structure for accounting and financial reporting.

**USA PATRIOT Act of 2001:** To deter and punish terrorist acts, to enhance law enforcement investigative tools, and for other purposes such as enhanced surveillance, monitoring foreign students, background checks, disclosure of educational records, and deterrence and prevention of cyberterrorism.

**The State of Texas Open Records Act:** Requires that all records of the executive and legislative branches of state and local government be made available for public examination unless the records fall within one of the exceptions listed in the statute. Examples of applicable exceptions are as follows.

- Information made confidential by law
- Working papers of the state auditors
- Private information in personnel files
- Student records
- Patient medical records

**Texas Administrative Code, Chapter 202 (Information Security Standards):** State legislative policy mandating computer security practices.

**Texas Government Code, Section 441:** Defines a state record and the requirements for records management.

**The State of Texas Penal Code, Chapter 33 (Computer Crimes) and Chapter 33A (Telecommunications Crimes):** A person commits an offense if the person...

- Knowingly accesses a computer, computer network, or computer system without the effective consent of the owner;
- Knowingly obtains a benefit, defrauds or harms another, or alters, damages, or deletes property;
- Knowingly and without authority uses or diverts telecommunications service; or,
- Knowingly obtains or attempts to obtain telecommunications service by a fraudulent or deceptive scheme, pretense, method, or conspiracy, or other device or means, including a false, altered, or stolen identification

**How You Can Help**

Ultimately, IR security is the user’s responsibility. You are responsible for all work done under your user ID and/or password. Therefore you, the user, must be alert to possible breaches in security and adhere to the security regulations that have been established within your area. The following list of security practices is not inclusive, but rather designed to raise your awareness towards protecting your information and information resources.

**Protect your area.**

- Keep unauthorized people AWAY from your equipment and data, challenge strangers in your area.
- UTMB personnel and visitors should wear identification badges in plain view at all times.
- Suspect any person who asks you to type a command.
- Verify caller identity before disclosing information over the telephone.
Use shredder or proper recycling receptacles in the disposal of all confidential and/or sensitive hardcopies.

- Keep keys under control.

Protect your equipment.

- Keep it in a secure environment.
- Keep food and drinks AWAY from it at all times.
- Know where the fire suppression equipment is and how to use it.

Protect your password.

- NEVER write it down or give it to anyone.
- Do not use names, numbers or dates which are personally identified with you.
- Change it often, but change it immediately if you think it has been compromised.

Protect your files.

- Understand the importance of your information and protect it accordingly.
- Control the use of sensitive systems.
- Do not allow unauthorized access to your files and data.
- NEVER leave your equipment unattended with your password activated - SIGN OFF!

Protect against viruses.

- Executable code should be scanned for viruses before you execute it, especially off of a floppy, CD, DVD or USB Storage device.
- Do not use shareware, freeware, software from home or a friend, unless it has been tested.

Protect your storage media.

- Protect sensitive data or information from casual viewing by others.
- Secure sensitive or critical information when not in use.
• Refuse to give system or site-related documentation to unknown persons.

Back up your data.
• Back it up as often as necessary, and always before implementing ANY new software.
• Keep duplicates of your sensitive data in a safe place, out of your immediate area.

Raise IR security consciousness.
• Make security of our information resources a part of your everyday life.
• Understand and comply with current security requirements.
• Encourage and support information resources security and training.
• Make suggestions for security improvements to the data owner or the ISO.
• Immediately report any unauthorized changes to your data.
• Immediately report any loss of information, whether automated or hardcopy.
• Immediately report any questionable usage of files, databases, or communication networks.

Failure to Comply (Individually)

Any event which results in theft, loss, unauthorized disclosure, unauthorized modification, or unauthorized destruction of IR constitutes a breach of security and confidentiality. Violations may include, but are not limited to, any act that:

• Exposes UTMB to actual or potential monetary loss through the compromise of IR security,
• Involves the disclosure of confidential information or the unauthorized use of UTMB data or resources,
• Involves the use of UTMB IR for personal gain, unethical, harmful, or illicit purposes, or
• Results in public embarrassment to UTMB.
Violation of this policy may result in immediate disciplinary action that may include, but may not be limited to:

- Formal reprimand,
- Suspended or restricted access to UTMB Information Resources,
- Restitution or reimbursement for any damage or misappropriation of UTMB property,
- Suspension without pay,
- Termination of employment,
- Termination of contract,
- Expulsion (permanent separation from the institution, as imposed by the Student Affairs Officer),
- Civil prosecution, or
- State and/or federal criminal prosecution.

**Failure to Comply (Institutionally)**

The chief administrative officer is responsible for ensuring that the state’s security and risk management policies are enforced. Should any audit indicate that the state’s security policies are not established or that the agency has not taken corrective action with respect to security deficiencies, the agency may be subject to any or all of the following:

- Further audit and review by the Office of the State Auditor,
- Disapproval by the DIR of agency strategic plans and/or agency operating plans, and/or
- Further action as deemed necessary by the DIR to ensure compliance with minimum security standards for protection of state information resources.
Conclusion

The statement that “IR security is everyone’s responsibility” is absolutely true. Each owner, custodian, and user of automated information assets has a personal responsibility to protect these resources. Functional managers have responsibility to provide appropriate security controls for any information resources entrusted to them. These managers are personally responsible for understanding the asset’s value and the extent of losses that could occur if the resources are not protected. Managers must ensure that all users of their data and systems are made aware of practices and procedures used to protect the information resources. When you don’t know what your security responsibilities are, ASK YOUR MANAGER.

Further References

For additional information, please refer to the individual policies in the following list as found in UTMB's Institutional Handbook of Operating Procedures…

2.13.2 Release of Information Under the Texas Open Records Act
2.19.5 Acceptable Use of Information Resources
2.19.6 Information Resources Security
2.19.7 Email Use
2.19.8 Internet Use
2.19.9 Utilizing Microcomputing Software in Compliance with Copyright Laws
2.27.7 Code of Ethics
7.1.3 Student Conduct and Discipline
9.2.11 Confidentiality of Patient Information

and as well, IR Security Practice Standards…

1.1.1 Security Monitoring
1.1.2 Intrusion Detection
1.1.3 Malware Detection
1.1.4 Network Configuration
1.1.5 Platform Hardening
1.1.6 Incident Management
1.2.1 Password Management
1.2.2 Account Management
1.2.3 Special Access
1.2.4 Vendor Access
1.2.5 Network Access
1.2.6 Physical Access
1.2.7 Wireless Access
1.3.1 Change Management
1.3.2 Backup/Data Recovery
1.4.1 Reporting of Lost or Stolen Information Resources and data

and also,

University of Texas System documents

UTS 165 Information Resource Use and Security Policy

published at http://cirt.utmb.edu/policies/policies.php

For additional information, contact:
the Information Security Officer,
Information Services, ext. 23838
THE UNIVERSITY OF TEXAS MEDICAL BRANCH
AT GALVESTON
INFORMATION RESOURCES SECURITY
ACKNOWLEDGMENT
AND NONDISCLOSURE AGREEMENT

Ensuring the security and integrity of the University of Texas Medical Branch at Galveston's information and information resources is the responsibility of all UTMB faculty, students and staff. The importance of protecting the reliability and accuracy of these information resources cannot be over emphasized. UTMB's academic, business, clinical, and research functions have become increasingly dependent on automation to access, process, store, and transmit information. The success of this university's missions depends on this information. The security and integrity of this information depend on each of us.

UTMB calls on all faculty, students and staff to fulfill the obligation of protecting these valuable information resources.

1. I understand and agree to abide by the following:

   a. ANY information concerning ANY person, system, or asset of UTMB that is obtained while performing my duties is of value to this university and may be confidential or sensitive, regardless of medium. I will NOT disclose any information to any individual, unless such release of information is directly related to the performance of my responsibilities.

   b. ALL passwords to information resources including, but not limited to, mainframe applications, network systems, voice mail, copy machines or long distance telephone use that I receive or devise are confidential and are to be used only by me. I will NOT disclose to any unauthorized person any password(s) I am given or devise and I will NOT write such password(s) or post them where they may be viewed by unauthorized persons. Use of a password not issued specifically to me or to a group of which I am a member is expressly prohibited. I am responsible for all transactions performed as a result of access authorized by use of my password.

   c. I will NOT attempt to circumvent the computer security system by using or attempting to use any transaction, software, files or resources that I am not authorized to use.

   d. I will NOT alter or in any way change information except in the performance of the duties of my job.
2. I understand and will comply with all policies, practice standards, and procedures adopted to safeguard information and associated information resources. Further, I acknowledge that I have received, read and understand the security policies outlined above and in the Information Resources Security Manual.

3. I understand that failure to comply with any of the conditions noted herein may result in my being disciplined or terminated from my position. I further understand that the university retains the right to pursue prosecution when misuse of its information and/or information resources is suspected.
Sign agreement, detach, and return to Access Management, Information Services, Route: 0849

UTMB INFORMATION RESOURCES SECURITY ACKNOWLEDGMENT AND NONDISCLOSURE AGREEMENT

My signature below represents my acknowledgment that I have received, read, and understand the security policies as outlined in the Information Resources Security Manual.

Name (print): ____________________________________________

Emp. No: _______________________________________________

Signature: ______________________________________________

Date: ___________________________________________________

Department: ____________________________________________
Attention: Access Management,
Information Services

Route: 0849