Information Resources Security

Definitions

Confidential Information: 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.

Custodian: An individual or entity responsible for implementing Owner-defined controls and access to an Information Resource. Custodians include Information Security Administrators, Entity information technology/systems departments, vendors, and any third party acting as an agent of or otherwise on behalf of an Entity.

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.

Information: Data organized, formatted and presented in a way that facilitates decision making. All information is data.

Information Resources (IR): any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistants (PDA), smart phones, 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 Manager (IRM): The IRM is responsible for management of all of the Entity’s information resources. The designation of an Entity information resources manager is intended to establish clear accountability for setting policy for information resources management activities, provide for greater coordination of the Entity’s information...
<table>
<thead>
<tr>
<th>Definitions, continued</th>
</tr>
</thead>
<tbody>
<tr>
<td>activities, and ensure greater visibility of such activities within and between Entities. The IRM has been given the authority and the accountability by the State of Texas to implement Security Policies, Procedures, Practice Standards and Guidelines to protect the Information Resources of the Entity including both central and decentralized areas. If an Entity does not designate an IRM, the title defaults to the institution’s president, and the president is responsible for adhering to the duties and requirements of an IRM.</td>
</tr>
</tbody>
</table>

**Information Security Officer (ISO):** responsible to the Information Resources Manager (IRM), and the Chief Business and Finance Officer for administering the information security functions within UTMB. The ISO is UTMB’s internal and external point of contact for all information security matters.

**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.

**Internet:** a global system interconnecting computers and computer networks. The computers and networks are owned separately by a host of organizations, government agencies, companies, and colleges. The Internet is the present “information super highway.”

**Intranet:** a private network for communications and sharing of information that, like the Internet, is based on TCP/IP, but is accessible only to authorized users within an organization. An organization’s intranet is usually protected from external access by a firewall.

**Owner:** The manager or agent responsible for the business function that is supported by the information 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 and authorizing access to the information resource. 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.
Definitions, continued

**President:** The President of UTMB

**Social Media**—any online networking service on which people publish, converse and share content from works of user-created video, audio, text or multimedia with the general public or with discreet groups of friends, colleagues or followers. Examples include but are not limited to: online posts/comments; media messaging service (MMS); Twitter®, Facebook®, LinkedIn®, YouTube® and all other social networks; and personal and organizational websites, blogs, wikis, and similar outlets.

**Policy**

The UTMB information resources infrastructure is an integrated network of computer resources which exists to support essential UTMB services and missions. This policy will address:

1. **Information Security**
   a. **Breach of confidential/protected data,**
   b. **Use of email,**
   c. **Use of the internet/intranet,**
   d. **Personal use of UTMB email, computers and other Information Resources**
   e. **Acquisition of hardware, software and peripherals**

Users are thus expected to exercise reasonable care in their use of this shared resource. Specifically included in this responsibility are:

- the observance of Federal, State, and Local laws and regulations governing the use of computing and network resources;
- the observance of all established policies and practice standards of UTMB
- the exercise of reasonable care to ensure that their use of these shared resources does not adversely impact availability of these same resources to other users; and the exercise of reasonable care to ensure the security of UTMB information resources.

Electronic files (including email) 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. Information Resources Standards and in the University of Texas SystemUTS-165 Information Resources Use and Security Policy.

As a user, it is also important to be aware that:

- no security mechanism is impregnable.
Policy, continued

- no security mechanism can protect against the improper behavior of authorized users

There is no guarantee of personal privacy. The use of electronic communications tools may be monitored to fulfill complaint or investigation requirements. 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.

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

Information Security

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.

1. UTMB IR users are required to protect confidential Digital Data (as defined by UTS 165, includes social security numbers, Protected Health Information (PHI), Confidential Research Data, digital Data associated with an individual and/or digital Data protected by law). Confidential digital Data must be secured and protected while at rest (electronic storage on a hard drive, digital or optical media), mobile (laptop, PDA or flash drive) and in transit (via email or the Internet). Users must report any weaknesses in UTMB computer security, and any incidents of possible misuse or violation of this agreement to the proper authorities by contacting the appropriate management or the UTMB Compliance Hotline at (800) 898-7679.

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

3. Users shall not share their UTMB account(s), passwords, Personal Identification Numbers (PIN), security tokens (e.g., Smartcard), or similar information or devices used for identification and authorization purposes. (Note: This is not applicable to the ‘delegation’ of access permissions; the intent is
Information Security, continued

to prohibit the literal shared use of access privileges via the same User ID and password).

4. If the computer system to which they are connected, or which they are currently using, contains confidential information or can be used to access other information resources on the UTMB network, users must not leave their microcomputer (PC), workstation or terminal unattended without first logging-out or invoking a password enabled screensaver, unless physical access is otherwise assured (e.g. a locked private office).

5. If there has been no activity on a computer terminal, workstation of microcomputer (PC) for 10 (ten) minutes, the system must automatically terminate the session or invoke a password enabled screensaver. Authentication to re-establish the session must occur after the lockout due to idle time.

6. Users shall not use non-standard software without initially contacting IS and receiving CIO/IRM approval unless it is on the UTMB standard software list.

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

8. Users shall not download, install or run security programs or utilities that reveal or exploit weaknesses in the security of a system. For example, UTMB users shall not run password cracking programs, packet sniffers, or port scanners or any other non-approved programs on UTMB IR.

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

10. Confidential data will not be stored on mobile computing devices (laptop computer, PDAs, Smart phones etc.) or mobile storage devices (USB drives, portable hard drives, etc.)

11. 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.

12. 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.
Breach of Security/Confidentiality

Any event that results in theft, loss, unauthorized use, unauthorized disclosure, unauthorized modification, unauthorized destruction, or degraded or denied services of IR constitutes a breach of security and/or confidentiality. This may include, but is not limited to, any act that:

1. exposes UTMB to actual or potential monetary loss through the compromise of IR security,
2. involves the disclosure of confidential information or the unauthorized use of UTMB data or resources
3. involves the use of UTMB IR for personal gain, unethical, harmful, or illicit purposes, or
4. results in public embarrassment to UTMB.

All breaches of security and/or confidentiality must be reported to the Office of Institutional Compliance or the Office of Information Security within 24 hours of discovery.

Use of Email

UTMB provides Email capability for legitimate business use in the course of assigned duties for the purpose of enhancing productivity and maintaining effective communications in support of the missions of UTMB.

The following activities represent a sample of prohibited email activities:

1. Email that is intimidating or harassing
2. Email that is used for personal profit
3. Email for purposes of political lobbying or campaigning
4. Email that violates copyright laws by inappropriately distributing protected works
5. Email that is likely to contain a computer virus
6. Use of Email to forward chain letters
7. Use of Email to send unsolicited messages to large groups except as required to conduct university business

Email containing confidential data which will be sent via a public network, such as the Internet, must be secured during transmission. Appropriate secure transmission methods include:

- Secured transmission channel (VPN or TLS-enabled transmission)
- Encrypted email
- Access controlled PDF
- Secure document collaboration software (e.g. iSpace)

Institutional backups are created solely for the purpose of restoring the...
Use of Email, continued

Entire electronic mail system in the event of disaster. Backups do not allow for the restoration of departmental electronic mail systems or individual mailboxes and cannot be used as a convenience to retrieve ‘deleted’ messages.

Backups do not serve a records retention function. Each UTMB department must make provisions to retain documents and messages in accordance with their departmental records retention policy.

Electronic mail is subject to the same records retention rules that apply to other documents and must be retained in accordance with departmental records retention schedules. The retention requirement associated with any document is determined by its content, not the method of delivery. See IHOP 2.1.4, Records and Information Management and Retention.

The responsibility of retaining an internally created and distributed documents (or messages) most often falls on the author – not the recipients.

Recipients may delete such as:

1. Received messages when their use has been fulfilled.
2. Most casual email messages are “transitory records” and can be discarded as their purpose is served.
3. For records retention purposes, electronic mail that is digitally signed must be filed electronically rather than on paper if the signature is of importance to the legal status or business usefulness of the document.
4. Email that has been requested in a subpoena or public information request must be retained until the request has been addressed, even if the retention period has expired.

Internet and Intranet Usage

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, UTS 165 - Information Resources Use and Security Policy

1. Software for browsing the Internet is provided to authorized users for business and research use only.
2. All software used to access the Internet must be part of the
Internet and Intranet Usage, continued

UTMB standard software suite or approved by the ISO. This software must incorporate all vendor provided security patches.

3. All files downloaded from the Internet must be scanned for viruses using the approved IS distributed software suite and current virus detection software.

4. All sites accessed must comply with the UTMB Acceptable Use Policies and Practice Standards.

5. All user activity on UTMB IR assets is subject to logging and review.

6. Content on all UTMB web sites must comply with the UTMB Acceptable Use Policies and Practice Standards.

7. No offensive or harassing material may be made available via UTMB web sites.

8. No personal commercial advertising may be made available via UTMB web sites.

9. UTMB Internet access may not be used for personal gain or non-UTMB personal solicitations.

10. No UTMB data will be made available via UTMB web sites without ensuring that the material is available to only authorized individuals or groups.

11. Posting confidential data to external, third-party websites must use Secure Socket Layer (SSL) protocols or other approved, secured transmission methods to protect the data in transit.

12. Electronic files are subject to the same records retention rules that apply to other documents and must be retained in accordance with department records retention schedules.

Personal Use of UTMB Email, Computers and other Information Resources

As a convenience to the UTMB user community, incidental use of IR is permitted. The following restrictions apply:

1. Incidental personal use of electronic mail, internet access, fax machines, printers, copiers, etc., is restricted to UTMB approved users, it does not extend to family members or other acquaintances.

2. Incidental use must not result in direct costs to UTMB.

3. Incidental use must not interfere with the normal performance of an employee’s work duties.

4. No files or documents may be sent or received that may cause legal action against, or embarrassment to, UTMB.

5. The use of, including downloading, storing or making available for upload, copyright materials (music, images, videos, etc.) must comply with applicable regulations, laws and UTMB policy.

6. Storage of personal email messages, voice messages, files and documents within UTMB’s IR should be nominal.
Personal Use of UTMB Email, Computers and other Information Resources, continued

| 7. | All messages, files and documents – including personal messages, files and documents – located on UTMB IR may be accessed in accordance with this policy. |
| 8. | May not be used for personal benefit/profit |
| 9. | All access to social networking sites must be done in accordance with IHOP 2.19.7, Use of Social Media |
| 10. | Users shall not intentionally access, create, store or transmit material which UTMB may deem to be offensive, indecent or obscene |

Acquisition of Hardware, Software, and Peripherals

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.

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, access to computer applications. To ensure a proper segregation of duties, owner responsibilities cannot be delegated to the custodian (e.g., Accounting, Invision, Pathology, Research Administrative Services, as owners, cannot delegate ownership responsibilities to Information Services, a custodian.)

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.

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.

The integrity of general use software, utilities, operating systems, networks, and respective data files are the responsibility of the custodian department.

Personally Identifiable or Protected Health Information used for test or
Acquisition of Hardware, Software, and Peripherals, continued

research purposes, must be de-identified in accordance with IHOP 6.2.29 and approved by the data owner or the Institutional Review Board, (whichever is applicable) prior to its use.

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.

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.

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.

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.

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.

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

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.

Volume licensed software products (such as Microsoft products provided through the Library Bookstore) provided to students, staff and faculty are provided to facilitate UTMB’s core functions and are for the use of the students, staff and faculty of UTMB Only. These licenses are invalid when the student, staff or faculty relationship with UTMB ends.
Acquisition of Hardware, Software, and Peripherals, continued

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.

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

References

- The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- Family Educational Rights and Privacy Act of 1974 (FERPA)
- The Copyright Act of 1976, as amended
- Texas Penal Code, Chapter 33 (Texas Computer Crimes Statute)
- Texas Penal Code, Chapter 33A (Telecommunications Crimes)
- Texas Administrative Code 1 TAC §202 (Information Security Standards)
- IHOP 2.19.7 Social Networking
- IHOP 6.2.29 - De-Identification of PHI
- IHOP 2.1.3 Release of Information Under the Texas Public Information Act
- IHOP 2.1.4 Records and Information Management
- IHOP 6.2.0 General Policy on the Use and Disclosure of PHI
- UTMB Information Resources Security Management Practice Standards
- The University of Texas System, UTS165 – Information Resources Use and Security Policy
- IHOP 3.5.4 Telecommuting (Alternate Work Site)